

# **Streaming von urheberrechtlich geschützten Werken**

Eine Bewertung aus der Perspektive des Schweizer  
Urheber- und Strafrechts

Dissertation  
der Rechtswissenschaftlichen Fakultät  
der Universität Zürich

zur Erlangung der Würde eines Doktors der Rechtswissenschaft

vorgelegt von

**Simon Jonas Böhi**

von Meilen ZH

genehmigt auf Antrag von

Prof. Dr. Christian Schwarzenegger  
und  
Prof. Dr. Florent Thouvenin

Die Rechtswissenschaftliche Fakultät gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 5. Oktober 2016

Die Dekanin: Prof. Dr. Brigitte Tag

Für meine Eltern



## **Vorwort**

Vorliegende Arbeit entstand während meiner Assistenzzeit am Lehrstuhl von Prof. Dr. Christian Schwarzenegger. Ihm möchte ich an dieser Stelle meinen herzlichen Dank aussprechen. Er hat mich auf das interessante Gebiet des Urheberstrafrechts aufmerksam gemacht und mir beim Verfassen der Arbeit grosse Freiheit gewährt. Bedanken möchte ich mich auch für die lehrreiche Zeit, die ich an seinem Lehrstuhl verbringen durfte.

Ebenfalls danke ich Prof. Dr. Florent Thouvenin, der das Erstellen des Zweitgutachtens übernommen hat.

Bedanken möchte ich mich weiter bei meinen Kollegen für die anregenden Diskussionen und wertvollen Denkanstösse. Ein besonderer Dank gebührt MLaw Carlo Hamburger und lic. iur. Simon Meier für die Durchsicht des Manuskripts.

Gewidmet ist die Arbeit meinen Eltern Elsbeth und Hannes Böhi, die mir meine Ausbildung ermöglicht und mich stets unterstützt haben.

Zürich im August 2015

SIMON J. BÖHI



## Inhaltsübersicht

Vorwort	V
Inhaltsübersicht	VII
Inhaltsverzeichnis	IX
Abkürzungsverzeichnis	XXII
Literaturverzeichnis	XXXI
Materialienverzeichnis	LV
Einleitung	1
I. Problemstellung und Zielsetzung	1
II. Gang der Untersuchung	2
1. Teil: Technische und rechtliche Grundlagen des Streaming	5
I. Technische Einführung	5
II. Urheberrechtsschutz	19
2. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Stream-Anbieters	29
I. Betroffene Verwertungsrechte	29
II. Illegale Streaming-Dienste (am Beispiel von <i>kino.to</i> )	45
III. Live-Streaming von urheberrechtlich geschützten Werken durch Private	68
3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers	73
I. Urheberrechtlich relevante Werknutzung oder bloss rezeptiver Werkgenuss?	73
	VII

## Inhaltsübersicht

---

II.	Schranken des Urheberrechts	81
III.	Technische Massnahmen zum Schutz digitaler Werke beim Streaming	100
4. Teil:	Sonderfall <i>P2P-Streaming</i>	153
I.	Rechtliche Bewertung des <i>P2P-Streaming</i> aus Sicht der Nutzer	154
II.	Rechtliche Bewertung des <i>P2P-Streaming</i> aus Sicht der übrigen Beteiligten	159
III.	Legale Nutzungsmöglichkeiten von <i>P2P-Streaming</i>	172
5. Teil:	Rechtsdurchsetzung bei Urheberrechtsverletzungen im Rahmen des Streaming	174
I.	<i>Datenbearbeitung zur Ermittlung von Urheberrechtsverletzern im Internet</i>	175
II.	Warnhinweismodell	193
III.	Entfernung urheberrechtsverletzender Inhalte durch <i>Hosting-Provider (take down)</i>	199
IV.	Verhinderung des erneuten Hochladens ( <i>stay down</i> )	202
V.	Zugangssperren durch <i>Access-Provider</i>	205
	Zusammenfassung wesentlicher Ergebnisse	213
I.	Streaming aus der Perspektive der Anbieter	213
II.	Streaming aus der Perspektive der Nutzer	215
III.	Technische Massnahmen zum Schutze digitaler Streaming-Angebote	217
IV.	P2P-Streaming	219
V.	Rechtsdurchsetzung bei Urheberrechtsverletzungen im Rahmen des Streaming	220
VI.	Der weitere Gesetzgebungsprozess seit Dezember 2015	224



# Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Inhaltsverzeichnis	IX
Abkürzungsverzeichnis	XXII
Literaturverzeichnis	XXXI
Materialienverzeichnis	LV
Einleitung	1
I. Problemstellung und Zielsetzung	1
II. Gang der Untersuchung	2
1. Teil: Technische und rechtliche Grundlagen des Streaming	5
I. Technische Einführung	5
1. Streaming von Audio-/Video-Dateien	5
A. Lineares Streaming	8
a) Live-Streaming	8
b) Near-on-Demand-Streaming	9
B. Nicht lineares Streaming (On-Demand-Streaming)	9
a) Verschiedene Arten des On-Demand-Streaming	11
aa) True-On-Demand-Streaming	11
bb) Progressive Download	11
cc) Progressive Download mit http-Pseudo-Streaming	12
b) Technische Umsetzung der Distribution der Inhalte beim On-Demand-Streaming	12
aa) Streaming von einem Web-Server	13
bb) Streaming von einem Streaming-Server	14
C. P2P-Streaming	15
a) Tracker-Verfahren	16
b) Dezentrales Verfahren	16
	IX

## Inhaltsverzeichnis

---

2. Streaming von Computerspielen	17
3. Streaming von Büchern	18
II. Urheberrechtsschutz	19
1. Rechtsquellen	19
A. Internationales Recht	19
B. Nationales Recht	19
2. Räumlicher Geltungsbereich des schweizerischen Urheberstrafrechts	20
3. Inhalt des Schweizer Urheberrechts	21
A. Schutzvoraussetzungen	21
B. Rechte des Urhebers	22
C. Verwandte Schutzrechte (Art. 33 ff. URG)	23
D. Schranken des Urheberrechts	24
E. Rechtsschutz	26
a) Zivilrechtlicher Schutz	26
b) Strafrechtlicher Schutz	27
2. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Stream-Anbieters	29
I. Betroffene Verwertungsrechte	29
1. Vervielfältigungsrecht (Art. 10 Abs. 2 lit. a URG)	29
A. Nicht-lineares Streaming	30
B. Lineares Streaming	30
a) Live-Streaming	30
b) Near-on-Demand-Streaming	31
2. Recht der Zugänglichmachung (Art. 10 Abs. 2 lit. c URG)	32
A. Nicht-lineares Streaming	32
B. Lineares Streaming	33
3. Senderecht (Art. 10 Abs. 2 lit. d URG)	33
A. Nicht-lineares Streaming	34
B. Lineares Streaming	34
4. Werkintegrität (Art. 11 URG)	34
5. Erschöpfungsgrundsatz (Art. 12 URG)	35
A. Allgemeines	35
B. Der Erschöpfungsgrundsatz im digitalen Umfeld	36
6. Zwischenergebnis	38

7. Sonderfall: <i>Framing</i>	39
A. Technische Einführung des <i>Framing</i>	39
B. Rechtliche Qualifikation des <i>Framing</i>	40
a) Vervielfältigungsrecht	40
b) Öffentliche Zugänglichmachung	41
II. Illegale Streaming-Dienste (am Beispiel von <i>kino.to</i> )	45
1. Übersicht	45
2. Strafbarkeit der <i>Uploader</i>	46
A. Unerlaubte Herstellung von Werkexemplaren	46
a) Objektiver Tatbestand	46
b) Subjektiver Tatbestand	47
c) Rechtswidrigkeit und Schuld	47
d) Gewerbsmässiges Handeln	47
B. Unerlaubte Zugänglichmachung	48
a) Objektiver Tatbestand	48
aa) Unrechtmässigkeit der Tathandlung	48
bb) Rechtmässiger Privatgebrauch	48
b) Subjektiver Tatbestand	49
c) Rechtswidrigkeit und Schuld	49
d) Gewerbsmässiges Handeln	49
3. Strafbarkeit der Betreiber von <i>Linksammlungen</i>	50
A. Alleintäterschaft	50
B. Mittelbare Täterschaft	51
C. Mittäterschaft	51
a) Objektiver Tatbestand	51
b) Subjektiver Tatbestand	53
c) Rechtswidrigkeit und Schuld	53
d) Gewerbsmässiges Handeln	53
D. Anstiftung	54
a) Objektiver Tatbestand	54
b) Subjektiver Tatbestand	55
c) Rechtswidrigkeit und Schuld	55
E. Gehilfenschaft zur unerlaubten Herstellung von Werkexemplaren auf den <i>Servern</i> der <i>Filehoster</i>	55
F. Gehilfenschaft zur unerlaubten Zugänglichmachung von Werken	56
a) Objektiver Tatbestand	56
b) Subjektiver Tatbestand	57
c) Rechtswidrigkeit und Schuld	57

4. Strafbarkeit der <i>Filehoster</i>	58
A. Alleintäterschaft	58
B. Mittäterschaft	59
a) Objektiver Tatbestand	59
b) Subjektiver Tatbestand	60
c) Rechtswidrigkeit und Schuld	60
d) Gewerbsmässiges Handeln	60
C. Anstiftung	61
D. Gehilfenschaft zur unerlaubten Herstellung von Werkexemplaren	61
a) Objektiver Tatbestand	61
b) Subjektiver Tatbestand	61
c) Rechtswidrigkeit und Schuld	62
E. Gehilfenschaft zur unerlaubten Zugänglichmachung von Werken	62
a) Objektiver Tatbestand	62
b) Subjektiver Tatbestand	63
c) Rechtswidrigkeit und Schuld	63
5. Strafbarkeit der Werbekunden auf illegalen Streaming-Diensten	63
A. Alleintäterschaft oder Mittäterschaft	63
B. Gehilfenschaft zur unerlaubten Herstellung und Zugänglichmachung von Werken	63
a) Objektiver Tatbestand	64
b) Subjektiver Tatbestand	64
c) Rechtswidrigkeit und Schuld	65
6. Beteiligung an einer kriminellen Organisation	65
III. Live-Streaming von urheberrechtlich geschützten Werken durch Private	68
1. Übersicht	68
2. Rechtliche Bewertung	69
A. Betroffene Verwertungsrechte	69
a) Vervielfältigungsrecht (Art. 10 Abs. 2 lit. a URG)	69
b) Senderecht (Art. 10 Abs. 2 lit. d URG)	70
c) Weitersenderecht (Art. 10 Abs. 2 lit. e URG)	70
B. Schrankenregelung	71

a) Schranke für technisch bedingte Vervielfältigungen ohne eigenständige wirtschaftliche Bedeutung (Art. 24a URG)	71
b) Schranke des Privatgebrauchs (Art. 19 Abs. 1 lit. a URG)	72
C. Urheberstrafrechtliche Konsequenzen	72
3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers	73
I. Urheberrechtlich relevante Werknutzung oder bloss rezeptiver Werkgenuss?	73
1. Umfang der Teilvervielfältigung	75
2. Bestandsdauer der Teilvervielfältigung	76
3. Schutzfähigkeit von Teilvervielfältigungen	77
II. Schranken des Urheberrechts	81
1. Schranke für technisch bedingte Vervielfältigungen ohne eigenständige wirtschaftliche Bedeutung (Art. 24a URG)	82
A. Vorübergehende flüchtige oder begleitende Vervielfältigung (lit. a)	83
B. Die Vervielfältigung ist integraler und wesentlicher Teil eines technischen Verfahrens (lit. b)	84
C. Ausschliesslich der Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder einer rechtmässigen Nutzung dienende Vervielfältigung (lit. c)	85
a) Privilegierung von Internetzugangsanbietern	85
b) Rechtmässige Nutzung	85
aa) Einwilligung des Rechteinhabers	85
bb) Vervielfältigung wird durch eine andere Schranke für erlaubt erklärt	86
cc) Rechtmässigkeit der Quelle	87
dd) Rechtmässigkeit der Nutzungshandlung	89
D. Die Vervielfältigung hat keine eigenständige wirtschaftliche Bedeutung (lit. d)	90
a) Möglichkeit der Erzielung zusätzlicher Einnahmen	91

b)	Möglichkeit einer quantitativ oder qualitativ anderen Nutzung	92
c)	Über die rechtmässige Nutzung hinausgehender wirtschaftlicher Nutzen aus Sicht des Rezipienten	93
d)	Ersatzlose Streichung des negativen Tatbestandserfordernisses der fehlenden eigenständigen wirtschaftlichen Bedeutung	94
2.	Schranke des Privatgebrauchs (Art. 19 Abs. 1 lit. a URG)	95
A.	Vervielfältigungen aus unrechtmässiger Quelle	96
B.	Zahlenmässige Beschränkung der Privatvervielfältigungen	98
C.	Zulässigkeit des Streaming gestützt auf die Schrankenregelung zum Privatgebrauch	98
3.	Vergütung für den Eigengebrauch (Art. 20 URG)	99
III.	Technische Massnahmen zum Schutz digitaler Werke beim Streaming	100
1.	Einleitung	100
2.	Technische Massnahmen	101
A.	Zugangsschranken	101
B.	Nutzungsschranken	102
3.	DRM-Systeme (DRMS)	102
4.	Rechtlicher Schutz technischer Massnahmen (Art. 39a URG)	105
A.	Allgemeines	105
B.	Umgehungsverbot (Abs. 1)	106
C.	Wirksame technische Massnahme (Abs. 2)	106
D.	Verbot von Vorbereitungshandlungen (Abs. 3)	107
E.	Vorbehalt erlaubter Verwendungen (Abs. 4)	108
5.	Verletzung des Schutzes von technischen Massnahmen und von Informationen für die Wahrnehmung von Rechten (Art. 69a URG)	111
A.	Allgemeines	111
B.	Umgehung technischer Massnahmen	111
C.	Beschaffung, Herstellung und Vertrieb von Vorrichtungen zur Umgehung technischer Massnahmen	112
D.	Gewerbsmässige Verletzung	113

6. Umgehung von Zugangsschranken bei kostenpflichtigen Streaming-Angeboten	113
A. Fallbeispiel	113
B. Umgehungshandlung	114
C. Rechtliche Bewertung der Umgehung von Zugangsschranken zur Entgeltsicherung nach URG	114
D. Rechtliche Bewertung der Umgehung von Zugangsschranken nach StGB	117
a) Unbefugte Datenbeschaffung (Art. 143 StGB)	117
b) Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143 <sup>bis</sup> StGB)	120
c) Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)	121
d) Erschleichen einer Leistung (Art. 150 StGB)	123
aa) Allgemeines	123
bb) Erschleichen	124
cc) Leistung	124
dd) Entgeltlichkeitserfordernis	125
ee) Öffentlichkeitserfordernis	126
ff) Vorsatz	126
e) Konkurrenzen der computerstrafrechtlichen Bestimmungen	127
7. Umgehung von Geo-Sperren	129
A. Technische Einführung	129
a) Netzinterne Kontrollmechanismen	130
b) Netzexterne Faktoren	131
B. Massnahmen zur Identitätsverschleierung	131
a) Anonymisierungsdienste	131
b) Proxy-Server	133
c) Virtual Private Network (VPN)	133
C. Rechtliche Bewertung der Umgehung von Geo-Sperren	134
a) Strafbarkeit der Umgehung von Geo-Sperren nach URG	134
aa) Geo-Sperren als wirksame technische Massnahmen i.S.v. Art. 39a Abs. 2 URG?	135
bb) Scheitern einer Strafbarkeit nach Art. 69a Abs. 1 lit. a URG	136
cc) Strafantragsberechtigung	137

b)	Strafbarkeit der Umgehung von Geo-Sperren nach StGB	137
aa)	Unbefugte Datenbeschaffung (Art. 143 StGB)	137
bb)	Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143 <sup>bis</sup> StGB)	137
cc)	Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)	138
dd)	Erschleichen einer Leistung (Art. 150 StGB)	138
ee)	Herstellen und Inverkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote (Art. 150 <sup>bis</sup> StGB)	138
c)	Fazit zur Umgehung von Geo-Sperren	139
8.	Herunterladen von Audio-/Video-Streams mittels Streamripper, Recorder-Software und Konvertierungsdiensten	139
A.	Technische Einführung	139
B.	Rechtliche Bewertung des Einsatzes von Konvertierungsdiensten und Aufnahmesoftware nach URG	140
a)	Unerlaubte Werkänderung	141
b)	Unerlaubte Herstellung von Werkexemplaren	141
c)	Verbot der Umgehung technischer Massnahmen	142
d)	Verbot von Vorbereitungshandlungen	143
e)	Analoge Lücke	145
C.	Rechtliche Bewertung des Einsatzes von Konvertierungsdiensten und Aufnahmesoftware nach StGB	147
a)	Unbefugte Datenbeschaffung (Art. 143 StGB)	147
b)	Betrügerischer Missbrauch einer Datenverarbeitungs-anlage (Art. 147 StGB)	148
c)	Erschleichen einer Leistung (Art. 150 StGB)	148
D.	Exkurs: Rechtliche Bewertung des Vertriebs von Umgehungswerkzeugen und der Erbringung von	



Dienstleistungen zur Umgehung technischer Massnahmen	149
a) Strafbarkeit nach URG	149
b) Strafbarkeit nach StGB	150
4. Teil: Sonderfall <i>P2P-Streaming</i>	153
I. Rechtliche Bewertung des <i>P2P-Streaming</i> aus Sicht der Nutzer	154
1. Unerlaubte Zugänglichmachung eines Werks	154
A. Objektiver Tatbestand	154
B. Subjektiver Tatbestand	156
C. Rechtswidrigkeit und Schuld	157
2. Unerlaubte Herstellung von Werkexemplaren	157
A. Objektiver Tatbestand	157
B. Subjektiver Tatbestand	158
C. Rechtswidrigkeit und Schuld	158
II. Rechtliche Bewertung des <i>P2P-Streaming</i> aus Sicht der übrigen Beteiligten	159
1. Strafbarkeit der Anbieter der <i>P2P-Streaming-Software</i>	159
A. Unerlaubte Zugänglichmachung des Werks	159
a) Alleintäterschaft	159
b) Mittelbare Täterschaft	160
c) Mittäterschaft	161
aa) Objektiver Tatbestand	161
bb) Subjektiver Tatbestand	162
cc) Rechtswidrigkeit und Schuld	163
dd) Gewerbsmässiges Handeln	163
d) Anstiftung	163
e) Gehilfenschaft	164
aa) Objektiver Tatbestand	164
bb) Subjektiver Tatbestand	165
cc) Rechtswidrigkeit und Schuld	166
B. Unerlaubte Herstellung von Werkexemplaren	166
a) Alleintäterschaft	166
b) Mittelbare Täterschaft	166
c) Mittäterschaft	166
aa) Objektiver Tatbestand	166
bb) Subjektiver Tatbestand	167

cc) Rechtswidrigkeit und Schuld	167
d) Anstiftung	167
e) Gehilfenschaft	167
aa) Objektiver Tatbestand	167
bb) Subjektiver Tatbestand	168
cc) Rechtswidrigkeit und Schuld	168
2. Strafbarkeit involvierter Anonymisierungsdienste	169
A. Mittäterschaft	169
B. Gehilfenschaft	169
a) Objektiver Tatbestand	169
b) Subjektiver Tatbestand	170
c) Rechtswidrigkeit und Schuld	171
3. Strafbarkeit der <i>Hosting-Provider</i>	171
A. Alleintäterschaft	171
B. Mittäterschaft	171
C. Gehilfenschaft	171
III. Legale Nutzungsmöglichkeiten von <i>P2P-Streaming</i>	172
5. Teil: Rechtsdurchsetzung bei Urheberrechtsverletzungen im Rahmen des Streaming	174
I. <i>Datenbearbeitung zur Ermittlung von Urheberrechtsverletzern im Internet</i>	175
1. Probleme bei der Ermittlung der Täterschaft bei Urheberrechtsverletzungen im Internet <i>de lege lata</i>	175
A. Anonymität im Internet	175
a) Der „Logistep-Entscheid“	176
aa) Empfehlung des EDÖB	177
bb) Entscheid des Bundesverwaltungsgerichts	178
cc) Entscheid des Bundesgerichts	179
b) Rechtslage nach dem Logistep-Entscheid gemäss dem EDÖB	181
c) Rechtslage nach dem Logistep-Entscheid gemäss dem Entscheid des Berner Obergerichts vom 22. März 2011	182
aa) Ausgangssachverhalt	182
bb) Entscheid des Berner Obergerichts	182

d)	Rechtslage nach dem Logistep-Entscheid gemäss dem Entscheid des Zürcher Obergerichts vom 3. Februar 2014	184
aa)	Ausgangssachverhalt	184
bb)	Entscheid des Zürcher Obergerichts	185
B.	Kritische Würdigung der Rechtslage beim Sammeln von <i>IP-Adressen de lege lata</i>	186
a)	IP-Adressen als Personendaten i.S.v. Art. 3 lit. a DSG	186
b)	Persönlichkeitsverletzung nach Art. 12 Abs. 2 lit. a DSG	187
c)	Rechtfertigungsgründe	188
2.	Neue gesetzliche Grundlagen für die Ermittlung der Täterschaft bei Urheberrechtsverletzungen im Internet <i>de lege ferenda</i>	189
II.	Warnhinweismodell	193
1.	Vorschlag der AGUR12	193
2.	Bisherige Erfahrungen mit einem Warnhinweismodell am Beispiel Frankreichs	194
3.	Kritische Würdigung der Einführung eines Warnhinweismodells	195
III.	Entfernung urheberrechtsverletzender Inhalte durch <i>Hosting- Provider (take down)</i>	199
1.	Vorschlag der AGUR12	199
2.	Bemerkungen	200
IV.	Verhinderung des erneuten Hochladens ( <i>stay down</i> )	202
1.	Vorschlag der AGUR12	202
2.	Bemerkungen	203
V.	Zugangssperren durch <i>Access-Provider</i>	205
1.	Vorschlag der AGUR12	205
2.	Technische Grundlagen	206
A.	DNS-Sperren	206
a)	Funktionsweise	206
b)	Umgehungsmöglichkeiten	207
B.	IP-Sperren	208
a)	Funktionsweise	208
b)	Umgehungsmöglichkeiten	209

3. Bemerkungen	209
A. Zuständigkeit	209
B. Vereinbarkeit von Zugangssperren mit den Grundrechten der Betroffenen	210
a) Genügende gesetzliche Grundlage	210
b) Öffentliches Interesse oder Schutz von Grundrechten Dritter	211
c) Verhältnismässigkeit	211
aa) Eignung	211
bb) Erforderlichkeit	212
cc) Verhältnismässigkeit im engeren Sinn (Zumutbarkeit)	212
Zusammenfassung wesentlicher Ergebnisse	213
I. Streaming aus der Perspektive der Anbieter	213
II. Streaming aus der Perspektive der Nutzer	215
III. Technische Massnahmen zum Schutze digitaler Streaming-Angebote	217
IV. P2P-Streaming	219
V. Rechtsdurchsetzung bei Urheberrechtsverletzungen im Rahmen des Streaming	220
VI. Der weitere Gesetzgebungsprozess seit Dezember 2015	224
1. Vorentwurf zur Änderung des URG	224
A. Teilnehmeridentifikation und Warnhinweismodell	224
B. Take down und stay down Pflicht für Hosting Provider	225
C. Netzsperrern	225
2. Ergebnis der Vernehmlassung und Kompromiss in der AGUR12 II	226
A. Mehr Pflichten für Hosting Provider	226
B. Datenbearbeitung zur strafrechtlichen Verfolgung von Urheberrechtsverletzungen im Internet	227
C. Abkehr von Netzsperrern und Warnhinweismodell	227
3. Gesetzesentwurf und Botschaft zur Revision des Urheberrechtsgesetzes	227
A. Stay down-Regel für gewisse Hosting Provider	227

B.	Bearbeitung von Personendaten zum Zweck der Strafantragstellung oder der Strafanzeigeerstattung	229
C.	Keine Netzsperrern und keine Kriminalisierung des Konsums illegaler Angebote	229
D.	Weitere Streaming-relevante Änderungen	230
a)	Video-on-Demand Vergütung für Urheber und Interpreten	230
b)	Verlängerung der Schutzfrist im Bereich der verwandten Schutzrechte	230
4.	Fazit zur Botschaft zur Revision des Urheberrechts	231

## Abkürzungsverzeichnis

A.	Auflage
a.A.	anderer Auffassung
ABl.	Amtsblatt (Europäische Union)
Abs.	Absatz
ACTA	Anti-Counterfeiting Trade Agreement
AG	Aktiengesellschaft
AGUR12	Arbeitsgruppe zur Optimierung der kollektiven Verwertung von Urheberrechten und verwandten Schutzrechten (einberufen am 8. August 2012)
AIPPI	Association Internationale pour la Protection de la Propriété intellectuelle
AJP	Aktuelle Juristische Praxis (Lachen)
a.M.	anderer Meinung
amtl.	amtliches
App	Applikation
Art.	Artikel
ASP	Application Service Provider
aStGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0) (Stand am 1. Oktober 2011)
AV	Audio/Video
Az.	Aktenzeichen
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
Beil.	Beilage
BGE	Entscheidungen des Schweizerischen Bundesgerichts, Amtliche Sammlung (Lausanne)
BGer	Bundesgericht
BGH	(deutscher) Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BK	Beschwerdekammer
BSK	Basler Kommentar
XXII	

bspw.	beispielsweise
Bull.	Bulletin
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000 (SR 780.1)
BV	Bundesverfassung
bzw.	beziehungsweise
CAN	Zeitschrift für kantonale Rechtsprechung (Zürich)
CaS	Causa Sport, Zürich
CCH	Code of Conduct Hosting
CD(s)	Compact Disc(s)
CDN	Content Distribution Network
CHF	Schweizer Franken
CP	Code pénal
CPI	Code de la propriété intellectuelle (créé par la loi no 92-597 du 1er juillet 1992, publié au JORF n° 153 du 3 juillet 1992; Frankreich)
CR	Computer und Recht (Köln)
DE	Bundesrepublik Deutschland
DeCSS	Decrypt Content Scrambling System
d.h.	das heisst
DHT(s)	Distributed hash table(s)
digma	Zeitschrift für Datenrecht und Informationssicherheit (Zürich)
Diss.	Dissertation
DNS	Domain Name Service
DPI	Deep Packet Inspection
DRM	Digital Rights Management
DRMS	Digital Rights Management System
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1)
DVD(s)	Digital Versatile Disc(s)
EC	Electronic Cash
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

## Abkürzungsverzeichnis

---

EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften/Europäische Gemeinschaft
eidg.	eidgenössischer
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EME	encrypted media extensions
Erkl.	Erklärung
Erw.	Erwägung
et al.	und andere
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (München)
e.V.	eingetragener Verein
f./ff.	und folgende (Seite/Seiten)
FAPL	Football Association Premier League
FMG	Fernmeldegesetz vom 30. April 1997 (SR 784.10)
Fn.	Fussnote
FP	forumpoenale (Bern)
FS	Festschrift
gl. M.	gleicher Meinung
GmbH	Gesellschaft mit beschränkter Haftung
GRUR	Zeitschrift für gewerblichen Rechtsschutz und Urheberrecht (München)
GRUR-Int.	Zeitschrift für gewerblichen Rechtsschutz und Urheberrecht. Internationaler Teil (München)
GRUR-Prax	Zeitschrift für gewerblichen Rechtsschutz und Urheberrecht. Praxis im Immaterialgüter- und Wettbewerbsrecht (München)
GRUR-RR	Zeitschrift für gewerblichen Rechtsschutz und Urheberrecht, Rechtsprechungs-Report (München)
GT	Gemeinsamer Tarif
GUID	Globally Unique Identifier
GVP	Gerichts- und Verwaltungspraxis
Habil.	Habilitationsschrift



---

HADOPI	Haute Autorité pour la diffusion des œuvres et la protection des droits sur l'Internet
HFR	Humboldt Forum Recht (Berlin)
h.L.	herrschende Lehre
Hrsg.	Herausgeber(in)
HTML5	Hypertext Markup Language 5
HTTP/http	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IANA	Internet Assigned Numbers Authority
i.c.	in casu
ICANN	Internet Corporation for Assigned Names and Numbers
i.d.R.	in der Regel
IEEE	Institute of Electrical and Electronics Engineers
IFPI	International Federation of the Phonographic Industry, London
IGE	Eidgenössisches Institut für Geistiges Eigentum (Bern)
i.H.v.	in Höhe von
IIC	International Review of Intellectual Property and Competition Law (Berlin)
Info-Richtlinie	Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, Abl. EG L 167 vom 22. Juni 2001, 10
Int.	International
IP	Internet Protocol
i.S.	im Sinne
i.S.v.	im Sinne von
IT	Information Technology
i.V.m.	in Verbindung mit
JORF	Journal Officiel de la République Française (Paris)
Jusletter	Jusletter (Bern)
KOBK	Koordinationsstelle zur Bekämpfung der Internetkriminalität

## Abkürzungsverzeichnis

---

K&R	Zeitschrift für Kommunikation und Recht (Frankfurt am Main)
LG	Landgericht (Deutschland)
lit.	litera
m.a.W.	mit anderen Worten
Mbps	Megabits per second
m.E.	meines Erachtens
medialex	Zeitschrift für Medienrecht. Revue de droit des médias (Bern)
Mio.	Million(en)
MMR	MultiMedia und Recht – Zeitschrift für Informations-, Telekommunikations- und Medienrecht (München)
MP3	Tondatenformat
MP4	Multimediales Containerformat für MPEG-4 Dateien
MPEG	Moving Picture Experts Group
m.w.H.	mit weiteren Hinweisen
N	Note
NJOZ	Neue Juristische Online-Zeitschrift (München)
NJW	Neue Juristische Wochenschrift (München)
NR	Nationalrat
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht (München)
NZZ	Neue Zürcher Zeitung (Zürich)
OGer	Obergericht
OLG	Oberlandesgericht (DE)
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (SR 220)
P2P	Peer-to-Peer
PC	Personal Computer
PK	Praxiskommentar
Pra	Die Praxis (Basel)
PS	partie spéciale

PVP	Protected-Video-Path
RAM	Random-Access Memory
RBÜ	Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst, revidiert in Paris am 24. Juli 1971 (SR 0.231.15)
RomA	Internationales Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendunternehmen (Rom-Abkommen) vom 26. Oktober 1961 (SR 0.231.171)
Rs.	Rechtssache
RTMPE	Real Time Messaging Protocol Encrypted
Rz.	Randziffer
SHK	Stämpflis Handkommentar
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht (Zürich)
simsa	Swiss Internet Industry Association
SIWR	Schweizerisches Immaterialgüter- und Wettbewerbsrecht (Basel)
SJZ	Schweizerische Juristenzeitung (Zürich)
s.o.	siehe oben
sog.	sogenannt
SR	Systematische Sammlung des Bundesrechts
SSL	Secure Sockets Layer
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)
StR	Ständerat
s.u.	siehe unten
SUISA	Schweizerische Gesellschaft der Urheber musikalischer Werke
temp	temporäre Datei
TCP	Transmission Control Protocol
TLS	Transport Layer Security

## Abkürzungsverzeichnis

---

TOR	The Onion Router
TRIPS	Agreement on Trade Related Aspects of Intellectual Property Rights (Abkommen über die Errichtung der Welt-handelsorganisation vom 15. April 1994 – Abkommen über handelsbezogene Aspekte der Rechte an geistigem Eigentum) (SR 0.632.20)
TU	Technische Universität
TV	Television
u.a.	unter anderem/unter anderen
UDP	User Datagram Protocol
UFITA	Archiv für Urheber-, Film-, Funk- und Theaterrecht (Bern)
UGC	User Generated Content (nutzergenerierte Inhalte)
URG	Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (SR 231.1)
UrhG	Urheberrechtsgesetz vom 9. September 1965 (BGBl. I, 1273; Deutschland)
URL	Uniform Resource Locator
URV	Verordnung vom 26. April 1993 über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsverordnung, URV) (SR 231.11)
USA	United States of America
u.U.	unter Umständen
UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (SR 241)
vgl.	vergleiche
Vorb.	Vorbemerkung
VPN	Virtual Private Network
vs.	versus
VStrR	Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (SR 313.0)
W3C	World Wide Web Consortium
WCT	WIPO-Urheberrechtsvertrag vom 20. Dezember 1996 (SR 0.231.151)
WEP	Wired Equivalent Privacy

WIPO	World Intellectual Property Organization (Genf)
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht (Heidelberg)
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPPT	WIPO-Vertrag über Darbietungen und Tonträger, Genf 1996
WTO	World Trade Organization
WWW	World Wide Web
XaaS	Everything as a Service
z.B.	zum Beispiel
ZfWG	Zeitschrift für Wett- und Glücksspielrecht (Köln)
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210)
Ziff.	Ziffer
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik (Kiel)
zit.	Zitiert
ZR	Blätter für Zürcherische Rechtsprechung (Zürich)
ZSR	Zeitschrift für Schweizerisches Recht (Basel)
ZStR	Zeitschrift für Strafrecht (Bern)
ZUM	Zeitschrift für Urheber- und Medienrecht (Baden-Baden)



## Literaturverzeichnis

- ADOLPHSEN, JENS/MAYER, DOMINIK/MÖLLER, FREDERIK, Massenabmahnungen im Urheberrecht – Ein Geschäftsmodell auf dem Prüfstand, NJOZ 2010, 2394
- ANGELOPOULOS, CHRISTINA, Are blocking injunctions against ISPs allowed in Europe? Copyright enforcement in the post-Telekabel legal landscape, GRUR-Int. 2014, 1089
- AREZZO, EMANUELA, Hyperlinks and Making Available Right in the European Union – What Future for the Internet after *Svensson*?, IIC 2014, 524
- ARI, MUKIT H., Computerspiele – Urheberrecht und Abgrenzung zu weiteren im Computerspielmarkt relevanten Immaterialgüterrechten, Zürich 2014, zugleich: Diss. Zürich 2012
- ARLT, CHRISTIAN, Digital Rights Management Systeme – Der Einsatz technischer Maßnahmen zum Schutz digitaler Inhalte, München 2006, zugleich: Diss. Göttingen 2005
- AUF DER MAUR, ROLF/KELLER, CLAUDIA, Privatkopie – Ein wohlverordnetes Recht? Eine Schrankenbestimmung als Spielball sich wandelnder Interessen, sic! 2004, 79
- BÄCKER, KERSTIN/HÖFINGER, FRANK MICHAEL, Online-Vertrieb digitaler Inhalte – Erstvertrieb, nachgelagerte Nutzungen und nachgelagerte Märkte, ZUM 2013, 623
- BALTISSER, ANNINA, Datenbeschädigung und Malware im Schweizer Strafrecht – Der Tatbestand des Art. 144<sup>bis</sup> StGB im Vergleich zu den Vorgaben der Cybercrime Convention der deutschen Regelung, Zürich 2013, zugleich: Diss. Zürich 2013
- BARRELET, DENNIS/EGLOFF, WILLI, Das neue Urheberrecht, Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, 3. A., Bern 2008
- BAUMGARTNER, TOBIAS, Privatvervielfältigung im digitalen Umfeld, Zürich, 2006, zugleich: Diss. Zürich 2006

- BECHTOLD, STEFAN, Urheber- und Markenrecht im digitalen Zeitalter, ZSR 134 (2015) II, Schweizerischer Juristentag 2015, 73 (zit. BECHTOLD, ZSR 2015 II)
- BECHTOLD, STEFAN, Das Urheberrecht und die Informationsgesellschaft [Copyright Law and the Information Society], in: Hilty, Reto M./Peukert, Alexander (Hrsg.), Interessenausgleich im Urheberrecht, Baden-Baden 2004, 67 (zit. BECHTOLD, Informationsgesellschaft)
- BECHTOLD, STEFAN, Vom Urheber- zum Informationsrecht, München 2002, zugleich: Diss. Tübingen 2001 (zit. BECHTOLD, Informationsrecht)
- BECKER, MAXIMILIAN, Zur Berechnung der zulässigen Zahl digitaler Privatkopien, ZUM 2012, 643
- BENABOU, VALÉRIE-LAURE, The Chase: The French Insight into the „Three Strikes“-System, in: Stamatoudi Irene (Hrsg.), Copyright Enforcement and the Internet, Alphen aan den Rijn 2010, 163
- BENHAMOU, YANIV, Dommages-intérêts suite à la violation de droits de propriété intellectuelle, Zürich 2013, zugleich: Diss. Zürich 2013
- BERANEK ZANON, NICOLE, Zivilrechtliche Haftung von Filehostern bei Urheberrechtsverletzungen nach Schweizer Recht, Jusletter IT vom 11. Dezember 2013
- BERANEK ZANON, NICOLE/DE LA CRUZ BÖHRINGER, CARMEN, Urheberrechtliche Beurteilung von IaaS- (und XaaS)- Cloud-Diensten für die betriebliche Nutzung gemäss Art. 19 URG, sic! 2013, 663
- BERGER, CHRISTIAN, Urheberrechtliche Erschöpfungslehre und digitale Informationstechnologie, GRUR 2002, 198 (zit. BERGER, GRUR 2002)
- BERGER, MATHIS, Entwicklungen im Immaterialgüterrecht / Le Point sur le droit de la propriété intellectuelle, SJZ 2007, 403 (zit. BERGER, SJZ 2007)
- BERGER, MATHIS, ASP: Ein neues Geschäftsmodell als Herausforderung für das Recht?, sic! 2002, 667 (zit. BERGER, sic! 2002)
- BIAGGINI, GIOVANNI, BV – Bundesverfassung der Schweizerischen Eidgenossenschaft, Zürich 2007
- BIELER, BRIGITTE, Anmerkungen zu Entscheid des Bundesgerichts vom 28. November 2014 „Bibliothekslieferdienst“, sic! 2015, 155



- BISGES, MARCEL, Voraussetzungen der Auskunft bei Providern über ihre Kunden anhand von IP-Adressen, *wistra* 2009, 303
- BORGHI, MAURIZIO, Chasing Copyright Infringement in the Streaming Landscape, *IIC* 2011, 316
- BORNHAUSER, JONAS, Anwendungsbereich und Beschränkung des urheberrechtlichen Vervielfältigungsrechts im digitalen Kontext, Bern 2010, zugleich: Diss. Zürich 2009
- BOSSHART, MELANIE, Das Creative-Commons-Lizenzsystem, Alternativer Verwertungsansatz für Rechte an geistigem Eigentum im digitalen Zeitalter, Zürich 2013, zugleich: Diss. Zürich 2013
- BOTT, KRISTOFER/CONRAD, ALBRECHT/BJÖRN, JOACHIM/NORDEMAN, JAN BERND/PILLA, MARCUS, Internationale Vereinigung für den Schutz des Geistigen Eigentums (AIPPI) – Berichte der Deutschen Landesgruppe für die Sitzung des Geschäftsführenden Ausschusses der AIPPI vom 13. bis 19. Oktober 2011 in Hyderabad, Indien, *GRUR-Int.* 2011, 905
- BÖTTCHER, HORST, Die urheberrechtliche Erschöpfung und ihre Bedeutung im digitalen Umfeld, Bern 2013, zugleich: Diss. Bern 2013
- BRÄNDLI, SANDRA/TAMÒ, AURELIA, Mainstream – Streaming als Nutzungsform der Gegenwart und der Zukunft, *sic!* 2013, 651
- BRÄNDLI, SANDRA/STRASZ, ANNA, Vergütung für den Privatgebrauch in der Schweiz und ausgewählten Staaten der EU – Wer schuldet wem wie viel?, in: Brändli Beat/Brändli Sandra, *Schriften der Assistierenden der Universität St. Gallen (HSG)*, Band 7: Schulden haben und machen – Auswirkungen auf Wirtschaft, Recht und Gesellschaft, St. Gallen 2012
- BRODKIN, JON, Netflix researching „large-scale peer-to-peer technology“ for streaming, 25. April 2014, <<http://arstechnica.com/information-technology/2014/04/netflix-researching-large-scale-peer-to-peer-technology-for-streaming>> (besucht 25. August 2015)
- BRÜGGEMANN, SEBASTIAN, Urheberrechtsdurchsetzung im Internet – Ausgewählte Probleme des Drittauskunftanspruchs nach § 101 UrhG, *MMR* 2013, 278

- BRUNOTTE, NICO, Urheberrechtliche Bewertung der Streamingportale – Unter besonderer Berücksichtigung der Schrankenbestimmungen zu ephemeren Vervielfältigungen und des digitalen Werkgenusses, Frankfurt am Main 2014, zugleich: Diss. Hannover 2014
- BU, YUANSHI, Die Schranken des Urheberrechts im Internet – Eine rechtsvergleichende Untersuchung des schweizerischen und chinesischen Urheberrechts, Bern 2004, zugleich: Diss. Bern 2004
- BÜHLER, LUKAS, Schweizerisches und internationales Urheberrecht im Internet, Freiburg 1999, zugleich: Diss. Freiburg 2004
- BUSCH, THOMAS, Zur urheberrechtlichen Einordnung der Nutzung von Streamingangeboten, GRUR 2011, 496
- BÜSCHER, MAREILE/MÜLLER, JUDITH, Urheberrechtliche Fragestellungen des Audio-Video-Streamings, GRUR 2009, 558
- CHERPILLOD, IVAN, Geltungsbereich, in: von Büren, Roland/David Lucas (Hrsg.), SIWR II/1, 3. A., Basel 2014, 14 (zit. CHERPILLOD, SIWR II/1)
- CHERPILLOD, IVAN, Schranken des Urheberrechts, in: von Büren, Roland/David Lucas (Hrsg.), SIWR II/1, 3. A., Basel 2014, 254 (zit. CHERPILLOD, SIWR II/1)
- CHERPILLOD, IVAN, La révision de la loi sur le droit d’auteur, Jusletter vom 11. Februar 2008 (zit. CHERPILLOD, Jusletter vom 11. Februar 2008)
- CORBOZ, BERNARD, Les infractions en droit suisse, Volume I, 3. A., Bern 2010
- COUSINS, BEN, Weapons of Mass Disruption #3: How and Why Consoles Will Die, 7. Januar 2015, <<http://kotaku.com/5973498/weapons-of-mass-disruption-3-how-and-why-consoles-will-die>> (besucht 25. August 2015)
- CSOPORT, DANIEL, Rechtsschutz für Kunstschaffende im schweizerischen und internationalen Urheberrecht, Diss. St. Gallen 2008
- DESSEMONTET, FRANÇOIS, Inhalt des Urheberrechts, in: von Büren, Roland/David Lucas (Hrsg.), SIWR II/1, 3. A., Basel 2014, 175 (zit. DESSEMONTET, SIWR II/1)
- DESSEMONTET, FRANÇOIS, Le droit d’auteur, Lausanne 1999 (zit., DESSEMONTET, droit d’auteur)

- DE WERRA, JACQUES, Défis du droit d’auteur dans un monde connecté – Perspective „Inside-Out“, sic! 2014, 194 (zit. DE WERRA, sic! 2014)
- DE WERRA, JACQUES, Téléchargement d’œuvres protégées: l’impunité maintenue?, medialex 2006, 171 (zit. DE WERRA, medialex 2006)
- DONATSCH, ANDREAS, Strafrecht III, Delikte gegen den Einzelnen, 10. A., Zürich/Basel/Genf 2013 (zit. DONATSCH, Strafrecht III)
- DONATSCH, ANDREAS/TAG, BRIGITTE, Strafrecht I, Verbrechenslehre, 9. A., Zürich 2013
- DONATSCH, ANDREAS/WOHLERS, WOLFGANG, Strafrecht IV, Delikte gegen die Allgemeinheit, 4. A., Zürich 2011
- DONATSCH, ANDREAS/SCHWARZENEGGER, CHRISTIAN/WOHLERS, WOLFGANG, Strafprozessrecht, 2. A., Zürich 2014
- DREIER, THOMAS/SCHULZE, GERNOT, UrhG. Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz. Kommentar, 4. A., München 2013
- DRAHEIM, YVONNE/LEHMANN, PHILIPP, Facebook & Co.: Aktuelle rechtliche Entwicklungen im Bereich Social Media – Urheberrecht/Allgemeines Persönlichkeits- und Äusserungsrecht, GRUR-Prax 2014, 427
- DROESE, LORENZ, Die Akteneinsicht des Geschädigten in der Strafuntersuchung vor dem Hintergrund zivilprozessualer Informationsinteressen, Zürich 2008, zugleich: Diss. Luzern 2007
- DUPUIS, MICHEL/GELLER, BERNARD/MONNIER, GILLES/MOREILLON, LAURENT/PIGUET, CHRISTOPHE/BETTEX, CHRISTIAN/STOLL, DANIEL (Hrsg.), Petit Commentaire CP, Basel, 2012 (zit. DUPUIS ET AL., Petit Commentaire CP, N xx zu Art. yy)
- DURNER, WOLFGANG, Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet?, ZUM 2010, 833
- DYENS, ALEXANDRE, Territorialité et ubiquité en droit pénal international suisse, Etude critique des art. 3 et 8 CPS – Enjeux théoriques et pratiques, en particulier en matière de criminalité économique et financière, Basel 2014, zugleich: Diss. Lausanne 2014
- EGLI, URS, Update IT-Recht, Jusletter vom 25. August 2014

- EGLOFF, WILLI, Bezahlter Download zum Eigengebrauch? – Zur Tragweite des neuen Art. 3<sup>bis</sup> URG, *medialex* 2011, 72 (zit. EGLOFF, *medialex* 2011)
- EGLOFF, WILLI, Revisionsbedarf beim urheberrechtlichen Eigengebrauch? – Zur Notwendigkeit eines Forschungsprivilegs, *medialex* 2006, 35 (zit. EGLOFF, *medialex*, 2006)
- EGLOFF, WILLI, Rundfunk im Internet? Zur urheberrechtlichen Qualifikation von Simulcasting und Webcasting, *sic!* 2005, 96 (zit. EGLOFF, *sic!* 2005)
- EICHELBERGER, JAN, Urheberrecht und Streaming, in: Leible, Stefan (Hrsg.), *Der Schutz des geistigen Eigentums im Internet*, Tübingen 2012, 17
- EISELE, JÖRG, *Computer- und Medienstrafrecht*, München 2013
- ENSTHALER, JÜRGEN, Streaming und Urheberrechtsverletzungen, *NJW* 2014, 1553
- FANGEROW, KATHLEEN/SCHULZ, DANIELA, Die Nutzung von Angeboten auf kino.to – Eine urheberrechtliche Analyse des Film-Streamings im Internet, *GRUR* 2010, 677
- FEDERRATH, HANNES, Technische Grundlagen von Auskunftsansprüchen, *ZUM* 2006, 434
- FEHLBAUM, PASCAL/LATTMANN, STEPHANIE S., Schranken und anwendbares Recht bei Urheberrechtsverletzungen auf dem Internet, *sic!* 2009, 370
- FETSCHERIN, MARC, DRM – eine erste Problemskizze, *Jusletter* vom 7. November 2005
- FITZNER, JULIA, Von Digital-Rights-Management zu Content Identification: Neue Ansätze zum Schutz urheberrechtlich geschützter Multimediawerke im Internet – Eine technische, ökonomische und rechtliche Analyse, Baden-Baden/Bern/München 2011, zugleich: Diss. München 2010
- FLECHSIG, NORBERT P./GABEL, DETLEV, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks, *CR* 1998, 351
- FORSTER, MATTHIAS, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB, Bern 2006, zugleich: Diss. St. Gallen 2006

- FOUNTOULAKIS, CRISTIANA/FRANCEY, JULIEN, La diligence d'un hébergeur sur Internet et la réparation du préjudice, *medialex* 2014, 175
- FRECH, PHILIPP, Zivilrechtliche Haftung von Internet Providern bei Rechtsverletzungen durch ihre Kunden, Zürich 2009, zugleich: Diss. St. Gallen 2009
- FREY, DIETER/RUDOLPH, MATTHIAS/OSTER, JAN, Internetsperren und der Schutz der Kommunikation im Internet, *MMR-Beilage* 2012, 1
- FREY, HARALD, Massenabmahnungen und Social Norm Backlash im Urheberrecht, *ZUM* 2014, 554
- FRÖHLICH-BLEULER, GIANNI, Urheberrechtliche Nutzungsbefugnisse des EDV-Anwenders, *AJP* 5/1995, 655
- FUCHS, STEFANIE/FARKAS, THOMAS, Kann der EUGH dem Paperboy das (Best)Water reichen?, *ZUM* 2015, 110.
- GALETZKA, CHRISTIAN/STAMER, ERIK, Streaming – aktuelle Entwicklungen in Recht und Praxis – Redtube, kinox.to & Co., *MMR* 2014, 292
- GASSER, CHRISTOPH, Der Eigengebrauch im Urheberrecht, Bern 1997, zugleich: Diss. Bern 1997
- GASSER, URS/BURKERT, HERBERT/THOUVENIN, FLORENT/NOLAN, CAROLINE, ICANN – Observations from an Information Law Perspective, in: Sethe, Rolf/Heinemann, Andreas/Hilty, Reto M./Nobel, Peter/Zäch, Roger (Hrsg.), *Kommunikation, Festschrift für Rolf H. Weber*, Bern 2011, 469
- GEIGER, CHRISTOPHE, Honourable Attempt but (ultimately) Disproportionately Offensive against Peer-to-Peer on the Internet (HADOPI) – A Critical Analysis of the Recent Anti-File-Sharing Legislation in France, *IIC* 2011, 457 (zit. GEIGER, *IIC* 2011)
- GEIGER, CHRISTOPHE, Irrtum: Schranken des Urheberrechts sind Ausnahmebestimmungen und sind restriktiv auszulegen, in: Berger, Mathis/Macciachini, Sandro, *Populäre Irrtümer im Urheberrecht*, Festschrift für Reto M. Hilty, Zürich 2008, 63 (zit. GEIGER, *FS-Hilty*)
- GESMANN-NUISSL, DAGMAR/WÜNSCHE, KAI, Neue Ansätze zur Bekämpfung der Internetpiraterie – ein Blick über die Grenzen, *GRUR-Int.* 2012, 225

- GILLIÉRON, PHILIPPE, Le monde de l'audiovisuel à l'ère numérique – enjeux juridiques, sic! 2009, 755 (zit. GILLIÉRON, sic! 2009)
- GILLIÉRON, PHILIPPE, Les liens hypertextes et le droit privé, sic! 2000, 755 (zit. GILLIÉRON, sic! 2000)
- GIRSBERGER, MICHAEL, Schutz von technischen Massnahmen im Urheberrecht, Die WIPO-Internetabkommen und deren Umsetzung in den Vereinigten Staaten, der Europäischen Union und der Schweiz, Bern 2007, zugleich: Diss. Luzern 2006
- GLARNER, ANDREAS, Werknutzung im digitalen Zeitalter – Strafrechtliche Betrachtungen zu Art. 19 Abs. 1 lit. a URG und zum Schutz technischer Massnahmen, sic! 2006, 641 (zit. GLARNER, sic! 2006)
- GLARNER, ANDREAS, Musikpiraterie im Internet – Urheberstrafrechtliche Betrachtungen, Bern 2002, zugleich: Diss. Zürich 2002 (zit. GLARNER, Musikpiraterie im Internet)
- GLARNER, ANDREAS/RÜFENACHT, KARIN, (Pyrrhus-)sieg für den Datenschutz, Jusletter vom 20. Dezember 2010
- GLESS, SABINE, Strafverfolgung im Internet, ZStrR 2012, 3
- GODENZI, GUNHILD, Private Beweisbeschaffung im Strafprozess – Eine Studie zu strafprozessualen Beweisverboten im schweizerischen und deutschen Recht, Zürich 2008, zugleich: Diss. Zürich 2008
- GRABER, CHRISTOPH, Beobachtungsstelle für technische Massnahmen im Urheberrecht – Erste Erfahrungen und Prüfung von Handlungsbedarf im Bereich der Wissenschaft, sic! 2010, 329
- GREENBERG, ANDY, Inside Popcorn Time, the piracy party Hollywood can't stop, 18. März 2015, <<http://www.wired.com/2015/03/inside-popcorn-time-piracy-party-hollywood-cant-stop>> (besucht 25. August 2015)
- GREVE, HOLGER, Access-Blocking – Grenzen staatlicher Gefahrenabwehr im Internet, Berlin 2012, zugleich Diss. Berlin 2012
- HÄFELIN, ULRICH/HALLER, WALTER/KELLER, HELEN, Schweizerisches Bundesstaatsrecht, 8. A., Zürich 2012

- HAUNREITER, DIEGO, Technologische Schutzmassnahmen im revidierten Urheberrechtsgesetz – Eine Antwort auf Krisen im Zeitalter der technischen Revolution, in: Auswirkungen von Krisen auf Wirtschaft, Recht und Gesellschaft, Bern 2009, 101
- HÄUPTLI, MATTHIAS, Vorübergehende Vervielfältigungen im schweizerischen, europäischen und amerikanischen Urheberrecht, Basel 2004, zugleich: Diss. Basel 2004
- HEID, VERONIKA, Die Haftung bei Urheberrechtsverletzungen im Netz – Zur Reichweite des § 97 UrhG, Baden-Baden 2013, zugleich Diss. Zürich 2012
- HEINEMEYER, DENNIS/KREITLOW, MATTHIAS, Umgehung technischer Schutzmassnahmen von Medienangeboten – Rechtmässige Nutzung von Streaming-Technologie und Wirksamkeit des RTMPE gem. § 95a UrhG, MMR 2013, 623
- HEINEMEYER, DENNIS/KREITLOW, MATTHIAS/NORDMEYER, ARNE/SABELLEK, ANDRÉ, Kampf gegen Filesharing als Modell verfehlter Mehrfachkompensation? Fragen zur Schadenshöhe, zu Gesamtschuldnern und Beweisen bei Tauschbörsen, MMR 2012, 279
- HENDEL, ARNDT CHRISTOPH, Die urheberrechtliche Relevanz des Hyperlinks, Embedded Content nach deutschem und europäischem Recht, ZUM 2014, 102
- HENNEMANN, MORITZ, Urheberrechtsdurchsetzung und Internet, Baden-Baden 2011, zugleich: Diss. Freiburg im Breisgau 2011
- HEWICKER, JOHANNES/MARQUARDT, INGA/NEURAUTER, SEBASTIAN, Der Abmahnkosten-Ersatzanspruch im Urheberrecht, NJW 2014, 2753
- HILGARD, MARK C. (Hrsg.), Kulturflatrate, Kulturwertmark oder Three strikes an you are out: Wie soll mit Kreativität im Internet umgegangen werden?, Göttingen 2013
- HILGERT, PETER/GRETH, RÜDIGER, Urheberrechtsverletzungen im Internet, München 2014
- HILGERT, PETER/HILGERT, SEBASTIAN, Nutzung von Streaming-Portalen – urheberrechtliche Fragen am Beispiel von Redtube, MMR 2014, 85
- HILTY, RETO M., Urheberrecht, Bern 2011 (zit. HILTY, Urheberrecht)

- HILTY, RETO M., Urheberrecht in der Informationsgesellschaft – Schweizer Recht vs. Europäische Vorgaben, sic! 2004, 966 (zit. HILTY, sic! 2004)
- HILTY, RETO M., Urheberrecht in der Informationsgesellschaft: „Wer will was von wem woraus“, ZUM 2003, 983 (zit. HILTY, ZUM 2003)
- HILTY, RETO M., Die Leistungsschutzrechte im schweizerischen Urheberrechtsgesetz, Symposium zum neuen schweizerischen Urheberrechtsgesetz, UFITA 1994, 85 (zit. HILTY, UFITA 1994)
- HOEREN, THOMAS, Sieben Beobachtungen und eine Katastrophe, sic! 2014, 212 (zit. HOEREN, sic! 2014)
- HOEREN, THOMAS, Geolokalisation und Glücksspielrecht (Teil 2), ZfWG 2008, 311 (zit. HOEREN, ZfWG 2008)
- HOEREN, THOMAS, Zoning und Geolocation – Technische Ansätze zu einer Reterritorialisierung des Internet, MMR 2007, 3 (zit. HOEREN, MMR 2007)
- HOEREN, THOMAS, Werbung im WWW – Aus der Sicht des neuen UWG, MMR 2004, 643 (zit. HOEREN, MMR 2004)
- HÖFINGER, FRANK MICHAEL, Anmerkung zu EuGH, Urteil vom 13. Februar 2014 – C-466/12 – Nils Svensson u.a./Retriever Sverige AB, ZUM 2014, 293
- HOFMANN, FRANZ, Die Haftung des Inhabers eines privaten Internetanschlusses für Urheberrechtsverletzungen Dritter – Eine Analyse der Rechtsprechung des Bundesgerichtshofs, ZUM 2014, 654
- HOHLWECK, MARTIN, „Even Heaven Cries“ – Eine rechtliche Zwischenbilanz von Filesharing-Verfahren, GRUR 2014, 940
- HOLZNAGEL, DANIEL, Zur Providerhaftung – Notice and Take-Down in § 512 U.S. Copyright Act, GRUR-Int. 2007, 971
- HUG, GITTI, Haftung der Median im Internetzeitalter, medialex 2014, 52
- HÜRLIMANN, DANIEL, Suchmaschinenhaftung – zivilrechtliche Verantwortlichkeit der Betreiber von Internetsuchmaschinen aus Urheber-, Marken-, Lauterkeits-, Kartell- und Persönlichkeitsrecht, Bern 2012, zugleich: Diss. Bern 2012
- HURTADO POZO, JOSÉ, Droit pénal, Partie spéciale, Zürich 2009 (zit. HURTADO POZO, PS)



- JANI, OLE/LEENEN, FREDERIK, EuGH: Zulässige Verlinkung auf frei zugänglich veröffentlichte Artikel, Nils Svensson u.a./Retriever Sverige, GRUR 2014, 360
- JANISCH, FABIAN/LACHENMANN, MATTHIAS, Unzulässiges Angebot eines Stream-Konverters – Aber keine generelle Unzulässigkeit, MMR-Aktuell 2013, 352345 (zit. JANISCH/LACHENMANN, MMR-Aktuell 2013)
- JANISCH, FABIAN/LACHENMANN, MATTHIAS, Konvertierung von Musikvideo-Streams in Audiodateien – Eine Analyse aus Sicht des deutschen Urheberrechts, MMR 2013, 213 (zit. JANISCH/LACHENMANN, MMR 2013)
- JOLLER, NATALIE ALEXIA, Neue audiovisuelle Nutzungsarten – Der Leistungsschutz der Interpreten, St. Gallen 2010, zugleich: Diss. St. Gallen 2010
- KAEMPF, MARKUS/BÜRGE, STEFAN, Aktuelle Entwicklungen in der Unionsrechtsprechung zum Immaterialgüterrecht, in: Epiney, Astrid/Diezig, Stefan (Hrsg.), Schweizerisches Jahrbuch für Europarecht/Annuaire suisse de droit européen 2013/2014, Zürich 2014
- KERNEN, ALEXANDER, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden, Jusletter vom 4. März 2013
- KNIES, BERNHARD, DeCSS – Oder: Spiel mir das Lied vom Code, ZUM 2003, 286
- KOCH, FRANK A., Der Content bleibt im Netz – Gesicherte Werkverwertung durch Streaming-Verfahren, GRUR 2010, 574
- KOHLI, THOMAS, „Lyrics Server“, sic! 2003, 960
- KROPP, JONATHAN, Die Haftung von Host- und Access-Providern bei Urheberrechtsverletzungen, Frankfurt am Main 2012, zugleich: Diss. Berlin 2012
- KÜHL, EIKE, Kampf gegen Streamingmühlen, 29. Oktober 2014, <[www.zeit.de/digital/internet/2014-10/kinox-streaming-illegal-razzia](http://www.zeit.de/digital/internet/2014-10/kinox-streaming-illegal-razzia)> (besucht 25. August 2015)
- KUNTZ, WOLFGANG, BITKOM: Videostreaming verändert Fernsehverhalten, MMR-Aktuell 2014, 363971

- KUROSE, JAMES F./ROSS, KEITH W., Computernetzwerke: Der Top-Down-Ansatz, 6. A., Hallbergmoos 2014
- LAUBER, ANNE/SCHWIPPS, KARSTEN, Das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, GRUR 2004, 293
- LEISTNER, MATTHIAS, Urheberrecht an der Schnittstelle zwischen Unionsrecht und nationalem Recht, GRUR 2014, 1145
- LEISTNER, MATTHIAS/GRISSE, KARINA, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 2), GRUR 2015, 105 (zit. LEISTNER/GRISSE, GRUR 2015)
- LEISTNER, MATTHIAS/GRISSE, KARINA, Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), GRUR 2015, 19 (zit. LEISTNER/GRISSE, GRUR 2015)
- LEUENBERGER, LENA, Quelles obligations pour les fournisseurs d'accès à Internet pour prévenir les violations de droits d'auteur?, sic! 2014, 721
- LONGOLIUS, NIKOLAI, Web-TV – AV-Streaming im Internet, Köln 2011
- LUXEM, REDMER, Digital Commerce: Electronic Commerce mit digitalen Produkten, Lohmar 2000, zugleich: Diss. Münster (Westfalen) 1999
- MARLY, JOCHEN, Bildschirmkopien, Cache-Kopien und Streaming als urheberrechtliche Herausforderungen, EuZW 2014, 616
- MAY, ELISA, Urheberstrafrecht und Streaming, Hamburg 2014, zugleich: Diss. Würzburg 2014
- MENN, ANNATINA, Interessenausgleich im Filmurheberrecht, Zürich 2008, zugleich: Diss. Zürich 2008
- METZGER, AXEL, EuGH: Keine Pflicht für Betreiber sozialer Netzwerke zu umfassenden Überwachungs- und Filtersystemen, GRUR 2012, 382 (zit. METZGER, GRUR 2012)
- METZGER, AXEL, Der Einfluss des EuGH auf die gegenwärtige Entwicklung des Urheberrechts, GRUR 2012, 118 (zit. METZGER, GRUR 2012)
- MEYER, EMANUEL/GOVONI, CARLO, Der Schutz technischer Massnahmen und Informationen für die Rechtswahrnehmung in: von Büren, Roland/David Lucas (Hrsg.), SIWR II/1, 3. A., Basel 2014, 413

- MOREILLON, LAURENT, Les nouveaux délits informatiques sur Internet, *medialex* 2001, 21
- MOSIMANN, PETER, Verwandte Schutzrechte, in: von Büren, Roland/David Lucas (Hrsg.), *SIWR* II/1, 3. A., Basel 2014, 329
- MUELLER, MILTON/KUEHN, ANDREAS/SANTOSO, STEPHANIE MICHELLE, Policing the Network: Using DPI for Copyright Enforcement, in: *Surveillance & Society*, 4 (2012), 348
- MUGGLI, SANDRA, Im Netz ins Netz – Pädokriminalität im Internet und der Einsatz von verdeckten Ermittlern und verdeckten Fahndern zu deren Bekämpfung, Zürich 2014, zugleich: Diss. Zürich 2013
- MÜLLER, BARBARA K./OERTLI, REINHARD, Urheberrechtsgesetz (URG): Bundesgesetz über das Urheberrecht und verwandte Schutzrechte: Mit Ausblick auf das EU-Recht, deutsches Recht, Staatsverträge und die internationale Rechtsentwicklung, Bern 2012 (zit. SHK URG)
- MÜLLER, STEFAN, Cloud und Privatkopie, *ZUM* 2014, 11
- NAZARI-KHANACHAYI, ARIAN, Access-Provider als urheberrechtliche Schnittstelle im Internet – Europarechtliche Vorgaben im Hinblick auf Zugangserschwerungsverfügungen und Lösungsansätze für das deutsche Recht *de lege ferenda*, *GRUR* 2015, 115
- NEFF, EMIL F./ARN, MATTHIAS, Erster Teil: Urheberrechtlicher Schutz der Software, in: von Büren, Roland/David, Lucas (Hrsg.), *Schweizerisches Immaterialgüter- und Wettbewerbsrecht*, Band II/2, Urheberrecht im EDV-Bereich, Basel 1998, 1
- NIGGLI, MARCEL ALEXANDER/WIPRÄCHTIGER, HANS (Hrsg.), *Strafgesetzbuch* II, Art. 1-110 StGB, *Basler Kommentar*, 3. A., Basel 2013 (zit. BSK StGB I)
- NIGGLI, MARCEL ALEXANDER/WIPRÄCHTIGER, HANS (Hrsg.), *Strafgesetzbuch* II, Art. 111-392 StGB, *Basler Kommentar*, 3. A., Basel 2013 (zit. BSK StGB II)
- NORDEMANN, JAN BERND, Anmerkung zu EuGH, Urteil vom 27. März 2014 – C-314/12 – UPC Telekabel Wien GmbH/Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH („Kino.to“), *ZUM* 2014, 499

- OBERGFELL, EVA INÉS, Expansion der Vorbeugemassnahmen und zumutbare Prüfpflichten von File-Hosting-Diensten, NJW 2013, 1995
- OĞLAKCIOĞLU, MUSTAFA TEMMUZ, Der Videostream und seine urheberstrafrechtliche Bewertung, ZIS 2012, 431
- OTT, STEPHAN, Die urheberrechtliche Zulässigkeit des Framing nach der BGH-Entscheidung im Fall „Paperboy“, ZUM 2004, 357
- PEUKERT, ALEXANDER, DRM: Ende der kollektiven Vergütung, sic! 2004, 749
- PFENNIG, GERHARD, Digital Rights Management Systeme aus der Sicht von Verwertungsgesellschaften, ZUM 2004, 198
- PFISTER, CHRISTA, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, Zürich 2008, zugleich: Diss. Zürich 2008
- PFITZMANN, ANDREAS/KÖPSELL, STEFAN/KRIEGELSTEIN, THOMAS, Sperrverfügungen gegen Access-Provider – Technisches Gutachten, TU Dresden, 22. Dezember 2006, abrufbar unter: <<http://tinyurl.com/Gutachten-Sperrverfuegungen>> (besucht 25. August 2015)
- PIERCE, DAVID, Twitter's Periscope App lets you livestream your world, 26. März 2015, <<http://www.wired.com/2015/03/periscope>> (besucht 25. August 2015)
- PLATZ, ERNST, Regelung technischer Schutzmassnahmen im revidierten URG – Welches sind die praktischen Auswirkungen der Unterstellung technischer Schutzmassnahmen unter das revidierte URG?, Jusletter vom 16. Juni 2008
- PLEISTER, CHRISTIAN C.-W./RUTTIG, MARKUS, Neues Urheberrecht – neuer Kopierschutz, Anwendungsbereich und Durchsetzbarkeit des § 95a UrhG, MMR 2003, 763
- PRILL, AILEEN, Webradio-Streamripping, Eine neue Form der Musikpiraterie? Eine Untersuchung des urheberrechtlichen Rahmens für Webradios und der Schranke der Privatkopie, Frankfurt am Main 2013, zugleich: Diss. Göttingen 2013
- PROBST, THOMAS, Die unbestimmte „Bestimmbarkeit“ der von Daten betroffenen Person im Datenschutzrecht, AJP 10/2013, 1423

- RADMANN, FRIEDRICH, Kino.ko – Filmegucken kann Sünde sein – Zur Rechtswidrigkeit der Nutzung von (offensichtlich) illegalen Streaming-Filmportalen, ZUM 2010, 387
- REDLICH, PHILIPP C., RedTube-Abmahnungen: Urheberrechtsverstoss durch Streaming?, K&R 2014, 73 (zit. REDLICH, K&R 2014)
- REDLICH, PHILIPP C., Download von Video- und Audiostreams zum privaten Gebrauch – eine „rechtliche Grauzone“, K&R 2012, 713 (zit. REDLICH, K&R 2012)
- REHBINDER, MANFRED, Tauschbörsen, Sharehoster und UGC-Streamingdienste – Tatsächliche und rechtliche Aspekte zur Piraterie im Netz, ZUM 2013, 241 (zit. REHBINDER, ZUM 2013)
- REHBINDER, MANFRED, Schweizerisches Urheberrecht, 3. A., Bern 2000 (zit. REHBINDER, Urheberrecht)
- REHBINDER, MANFRED/VIGANÒ, ADRIANO (Hrsg.), Urheberrecht und verwandte Schutzrechte mit ausführenden Verordnungen, Nebengesetzen, zwischenstaatlichen Verträgen (insbesondere WIPO- und TRIPS-Abkommen, RBÜ und Rom-Abkommen), weiteren Materialien sowie Sachregister, 3. A., Zürich 2008
- REINBACHER, TOBIAS, Zur Strafbarkeit der Betreiber und Nutzer von Kino.to, NStZ 2014, 57 (zit. REINBACHER, NStZ 2014)
- REINBACHER, TOBIAS, Zur Strafbarkeit des Streaming und der Umgehung von Geo-IP-Sperren durch private Nutzer, HFR 2012, 179 (zit. REINBACHER, HFR 2012)
- REINEMANN, SUSANNE/REMMERTZ, FRANK, Urheberrechte an User-generated Content, ZUM 2012, 216
- REUSSER, STEVE, L’admissibilité des hyperliens en droit d’auteur, Basel 2014, zugleich: Diss. Neuchâtel 2014
- REUSSER, STEVE, L’admissibilité des hyperliens en droit d’auteur européen, Jusletter vom 28. April 2014
- RIEDO, CHRISTOF, Der Strafantrag, Basel 2004, zugleich: Diss. Freiburg 2004.

- RIGAMONTI, CYRILL P., Urheberpersönlichkeitsrechte – Globalisierung und Dogmatik einer Rechtsfigur zwischen Urheber- und Persönlichkeitsrecht, Bern 2013, zugleich: Habil. Bern 2013 (RIGAMONTI, Urheberpersönlichkeitsrechte)
- RIGAMONTI, CYRILL P., Zur Zulässigkeit des Handels mit Softwareproduktschlüsseln, AJP 5/2010, 582 (zit. RIGAMONTI, AJP 2010)
- RIGAMONTI, CYRILL P., Der Handel mit Gebrauchtssoftware nach schweizerischem Urheberrecht, GRUR-Int. 2009, 14 (zit. RIGAMONTI, GRUR-Int. 2009)
- RIGAMONTI, CYRILL P., Eigengebrauch oder Hehlerei? Zum Herunterladen von Musik- und Filmdateien aus dem Internet, GRUR-Int. 2004, 278 (zit. RIGAMONTI, GRUR-Int. 2004)
- ROHN, PATRICK, Zivilrechtliche Verantwortlichkeit der Internetprovider nach schweizerischem Recht, Zürich 2004, zugleich: Diss. Zürich 2004
- ROSENTHAL, DAVID, „Logistep“: Offenbar ein Einzelfallentscheid, digma 2011, 40 (zit. ROSENTHAL, digma 2011)
- ROSENTHAL, DAVID, Wenn Datenschutz übertrieben wird oder: Hard cases make bad law, Jusletter vom 27. September 2010 (zit. ROSENTHAL, Jusletter vom 27. September 2010)
- ROSENTHAL, DAVID, Zivilrechtliche Haftung von Internet-Providern für Unrecht Dritter, sic! 2006, 511 (zit. ROSENTHAL, sic! 2006)
- RUBLI, DOMINIK P., Das Verbot der Umgehung technischer Massnahmen zum Schutz digitaler Datenangebote, Bern 2009, zugleich: Diss. Zürich 2009
- RUDIN, BEAT, „Personendaten“: ein Begriff in Anfechtung, digma 2011, 144
- RUNGE, PHILIPP, Die Vereinbarkeit einer Content-Flatrate für Musik mit dem Drei-Stufen-Test, GRUR-Int. 2007, 130
- SCHACK, HAIMO, Rechtsprobleme der Online-Übermittlung, GRUR 2007, 639 (zit. SCHACK, GRUR 2007)
- SCHACK, HAIMO, Private Vervielfältigung von einer rechtswidrigen Vorlage?, in: Ahrens, Hans-Jürgen et al. (Hrsg.), Festschrift für Willi Erdmann, Köln 2002, 165 (zit. SCHACK, FS-Erdmann)

- SCHACK, HAIMO, Schutz digitaler Werke vor privater Vervielfältigung – zu den Auswirkungen der Digitalisierung auf § 53 UrhG, ZUM 2002, 497 (zit. SCHACK, ZUM 2002)
- SCHÄFER, MARC-FRÉDÉRIC/DORDI, ELSA, Über die Rechtfertigung von Persönlichkeitsverletzungen, medialex 2011, 142
- SCHAPIRO, LEO/JENSSEN, LARS, Anmerkung zu BGH, Beschluss vom 16. Mai 2013 – I ZR 46/12 – Die Realität, ZUM 2013, 665
- SCHÄUFELE, MAXIMILIAN, Zur Strafbarkeit des Raubkopierens im Internet – Filesharing von urheberrechtlich geschützten Werken im Internet, Berlin/Münster 2013, zugleich: Diss. Heidelberg 2012
- SCHEDER-BIESCHIN, FELIX, Modernes Filesharing – Störerhaftung und Auskunftspflicht von Anonymisierungsdiensten, Edeweicht 2014, zugleich: Diss. München 2013
- SCHIPPAN, MARTIN, Rechtsfragen bei der Implementierung von Digital Rights Management-Systemen, ZUM 2004, 188
- SCHMID, NIKLAUS, Computer- sowie Check- und Kreditkarten-Kriminalität – Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994
- SCHMIDT-WUDY, FLORIAN, EuGH: Urheberrecht – Verweis auf geschützte Werke durch Hyperlinks keine öffentliche Wiedergabe, EuZW 2014, 265
- SCHREINER, RÜDIGER, Computernetzwerke – Von den Grundlagen zur Funktion und Anwendung, 5. A., München 2014
- SCHULDT, RAINER, Readfy: Werbefinanzierte Lese-App im Praxis-Test, 30. September 2014, <<http://www.computerbild.de/artikel/cb-News-App-Check-Readfy-eBooks-lesen-zum-Nulltarif-9906451.html>> (besucht 25. August 2015)
- SCHULZ, DANIELA, Der Bedeutungswandel des Urheberrechts durch Digital Rights Management – Paradigmenwechsel im deutschen Urheberrecht?, GRUR 2006, 470
- SCHULZE, GERNOT, Svensson, BestWater und Die Realität – Ist Framing nun grundsätzlich zulässig?, ZUM 2015, 106 (zit. SCHULZE, ZUM 2015)

- SCHULZE, GERNOT, Werkgenuss und Werknutzung in Zeiten des Internets, NJW 2014, 721 (zit. SCHULZE, NJW 2014)
- SCHWARTMANN, ROLF, Warnhinweise zur Sicherung von Urheberrechten im Internet – Das vorgerichtliche Mitwirkungsmodell im internationalen Kontext, GRUR-Prax 2012, 158
- SCHWARZENEGGER, CHRISTIAN, Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik – Cyberkriminalität und das neue Urheberstrafrecht, ZSR 127 (2008) II, Heft 2, 399 (zit. SCHWARZENEGGER, ZSR 2008 II)
- SCHWARZENEGGER, CHRISTIAN, Urheberstrafrecht und Filesharing in P2P-Netzwerken – Die Strafbarkeit der Anbieter, Downloader, Verbreiter von Filesharing-Software und Hash-Link-Setzer, in: Schwarzenegger Christian/Arter, Oliver/Jörg, Florian S. (Hrsg.), Internet-Recht und Strafrecht (4. Tagungsband, Bern 2005, 205 (zit. SCHWARZENEGGER, P2P-Netzwerke)
- SCHWARZENEGGER, CHRISTIAN, Sperrverfügungen gegen Access-Provider – Über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Arter, Oliver/Jörg, Florian S. (Hrsg.), Internet-Recht und Electronic Commerce Law, Bern 2003, 249 (zit. SCHWARZENEGGER, Sperrverfügungen)
- SCHWARZENEGGER, CHRISTIAN, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001 - Am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Fernmeldegeheimnisses, in: Donatsch, Andreas/Forster Marc/Schwarzenegger Christian (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel, Zürich 2002, 305 (zit. SCHWARZENEGGER, FS-Trechsel)
- SCHWARZENEGGER, CHRISTIAN, E-Commerce – Die strafrechtliche Dimension, in: Arter, Oliver/Jörg, Florian S. (Hrsg.), Internet-Recht und Electronic Commerce Law, Lachen/St. Gallen, 2001, 329 (zit. SCHWARZENEGGER, E-Commerce)
- SCHWARZENEGGER, CHRISTIAN, Abstrakte Gefahr als Erfolg im Strafanwendungsrecht – Ein leading case zu grenzüberschreitenden Internetdelikten, sic! 2001, 240 (zit. SCHWARZENEGGER, sic! 2001)



- SCHWARZENEGGER, CHRISTIAN, Gefangen im Spinnennetz der Strafjustiz? Die strafrechtliche Bewertung von Links, NZZ vom 30. Juni 2000, Nr. 150, 71 (zit. SCHWARZENEGGER, NZZ)
- SCHWARZENEGGER, CHRISTIAN, Der räumliche Geltungsbereich des Strafrechts im Internet – Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 2000, 109 (zit. SCHWARZENEGGER, ZStrR 2000)
- SCHWARZENEGGER, CHRISTIAN/NIGGLI, MARCEL ALEXANDER, Über die Strafbarkeit des Hyperlink-Setzers, medialex 2003, 26
- SCHWEINGRUBER, SANDRA, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10. November 2014
- SCHWEIZER, RAINER J., in: Ehrenzeller, Bernhard/Mastronardi, Philippe/Schweizer, Rainer J./Vallender, Klaus A. (Hrsg.), Die Schweizerische Bundesverfassung – Kommentar, 2. A., Zürich/St. Gallen 2008
- SCHWEIZER, RAINER J./BISCHOF, SEVERIN, Der Begriff der Personendaten – Herausforderungen an die Rechtsetzung und Rechtsprechung im kommunikationstechnologischen Umfeld, digma 2011, 152
- SCHWERZMANN, JACQUELINE, Kartellrechtlicher Schutz vor technischen Schutzmassnahmen?, sic! 2004, 148
- SEMADENI, THOMAS, Erschöpfungsgrundsatz im Urheberrecht, Bern 2004, zugleich: Diss. Zürich 2004
- SHAW, LUCAS/KHARIF, OLGA, Twitter's Periscope Responds to „Game of Thrones“ Piracy Reports, 13. April 2015, <<http://www.bloomber.com/news/articles/2015-04-13/twitter-s-periscope-responds-to-game-of-thrones-piracy-reports>> (besucht 25. August 2015)
- SOBIRAJ, LARS, Popcorn-time übernimmt den Markt, 10. Juli 2014, <<https://tarnkappe.info/popcorn-time-dominiert-den-markt-bittorrent-al-s-streaming-getarnt>> (besucht 25. August 2015)
- SOLMECKE, CHRISTIAN, Der Redtube-Fall – Eine Streaming-Abmahnwelle mit Risiken und Nebenwirkungen, CR 2014, 137
- SOLMECKE, CHRISTIAN/SEBASTIAN, MAIK/SAHUC, FRANCOIS-XAVIER, Experiment Internetsperre – Das erste Jahr des Hadopi-Gesetzes, MMR-Aktuell 2011, 316298

- SPINDLER, GERALD, Die Reform des Urheberrechts, NJW 2014, 2550 (zit. SPINDLER, NJW 2014)
- SPINDLER, GERALD, Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil „UPC Telekabel“, GRUR 2014, 826 (zit. SPINDLER, GRUR 2014)
- SPINDLER, GERALD, Streaming, Internetradios und Content-Portale im Urheber- und Medienrecht, in: Heinemann, Andreas/Hilty, Reto M./Nobel, Peter/Sethe, Rolf/Zäch, Roger (Hrsg.), Kommunikation, Festschrift für Rolf H. Weber, Bern 2011, 781 (zit. SPINDLER, FS-Weber)
- STADLER, THOMAS, Sperrverfügungen gegen Access-Provider, MMR 2002, 343
- STAUFFACHER, WERNER, Revision des Urheberrechtsgesetzes 2008 - praktische Konsequenzen im Kunstbereich, AJP 8/2008, 1255 (zit. STAUFFACHER, AJP 2008)
- STEIER, HENNING, Hornet statt Tor-Netzwerk, 27. Juli 2015, <<http://www.nzz.ch/hornet-statt-tor-netzwerk-ld.1180>> (besucht 25. August 2015) (zit. STEIER, Hornet)
- STEIER, HENNING, Periscope statt Pay-TV, 4. Mai 2015, <<http://www.nzz.ch/digital/boxkampf-floyd-mayweather-jr-und-manny-pacquiao-periscope-meerkat-1.18535113>> (besucht 25. August 2015) (zit. STEIER, Periscope)
- STEIER, HENNING, Popcorn Time will sich unangreifbar machen, 20. März 2015, <<http://www.nzz.ch/digital/popcorn-time-peer-to-peer-bittorrent-1.18506299>> (besucht 25. August 2015) (zit. STEIER, Popcorn Time)
- STEIER, HENNING, Netflix für Piraten ist wieder da, 17. März 2014, <<http://www.nzz.ch/digital/popcorn-time-yts-github-1.18264598>> (besucht 25. August 2015) (zit. STEIER, Netflix für Piraten)
- STEINHAUS, INGO, Readfys Streaming-Romane, 2. Februar 2014, <<http://digital-heartland.de/readfys-streaming-romane>> (besucht 25. August 2015)
- STIEPER, MALTE, Rezeptiver Werkgenuss als rechtmässige Nutzung - Urheberrechtliche Bewertung des Streaming vor dem Hintergrund des EuGH-Urteils in Sachen FAPL/Murphy, MMR 2012, 12

- STÖCKER, CHRISTIAN, Streaming-Software Popcorn Time: Schick, hip, illegal, 17. März 2014, <<http://www.spiegel.de/netzwelt/web/streaming-software-popcorn-time-schick-hip-illegal-a-959089.html>> (besucht 25. August 2015)
- STOLZ, ALEXANDER, Rezipient = Rechtsverletzer...? – (Keine) Urheberrechtsverletzung durch die Nutzung illegaler Streaming-Angebote, MMR 2013, 353
- STRAUB, WOLFGANG, Softwareschutz – Urheberrecht, Patentrecht, Open Source, Zürich 2011
- STRATENWERTH, GÜNTER, Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 4. A., Bern 2011
- STRATENWERTH, GÜNTER/WOHLERS, WOLFGANG, Schweizerisches Strafrecht, Handkommentar, 3. A., Bern 2013
- STRATENWERTH, GÜNTER/BOMMER, FELIX, Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 7. A., Bern 2013
- STRATENWERTH, GÜNTER/JENNY, GUIDO/BOMMER, FELIX, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 7. A., Bern 2010
- STRÖMER, TOBIAS H./GASPERS, HOLGER, „Umgehen“ des Kopierschutzes nach neuem Recht, K&R 2004, 14
- STROWEL, ALAIN, The „Graduated Response“ in France – Is It the Good Reply to Online Copyright Infringements?, in: Stamatoudi, Irene (Hrsg.), Copyright Enforcement and the Internet, Alphen aan den Rijn 2010, 147
- TANENBAUM, ANDREW S./WETHERALL, DAVID J., Computernetzwerke, 5. A., München 2012
- THIESEN, MICHAEL, Wie hoch ist der Preis der Anonymität? Haftungsrisiken beim Betrieb eines TOR-Servers, MMR 2014, 803
- THOUVENIN, FLORENT, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Weber, Rolf H./Thouvenin, Florent, Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 61 (zit. THOUVENIN, Big Data)

- THOUVENIN, FLORENT, Durchsetzung von Urheberrechten und Datenschutz, Lehren aus dem Scheitern von ACTA, in: Weber, Rolf H./Thouvenin, Florent, Neuer Regulierungsschub im Datenschutzrecht?, Zürich 2012, 105 (zit. THOUVENIN, ACTA)
- THOUVENIN, FLORENT, Urheberrecht statt „geistiges Eigentum“, NZZ vom 21. August 2012, Nr. 193, 19 (zit. THOUVENIN, NZZ)
- THOUVENIN, FLORENT, Offenlegung von Verbindungsdaten: Wenig Neues vom EuGH, Urteil des EuGH vom 29. Januar 2008, Rs. C-275/06, sic! 2009, 100 (zit. THOUVENIN, sic! 2009)
- THOUVENIN, FLORENT, Irrtum: Je kleiner der Gestaltungsspielraum, desto eher sind die Schutzvoraussetzungen erfüllt, in: Berger, Mathis/Macciachini, Sandro, Populäre Irrtümer im Urheberrecht, Festschrift für Reto M. Hilty, Zürich 2008, 63 (zit. THOUVENIN, FS-Hilty)
- TRECHSEL, STEFAN/PIETH, MARK (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 2. A., Zürich/St. Gallen 2013 (zit. PK StGB)
- ULLRICH, JAN NICOLAUS, Webradioportale, Embedded Videos & Co. – Inline Linking und Framing als Grundlage urheberrechtlich relevanter (Anschluss-)Wiedergaben, ZUM 2010, 853
- VAN DER SAR, ERNESTO, Netflix needs Bittorrent expert to implement P2P streaming, 20. Mai 2015, <<https://torrentfreak.com/netflix-needs-bittorrent-expert-to-implement-p2p-streaming-150520/>> (besucht 25. August 2015) (zit. VAN DER SAR, P2P-Streaming)
- VAN DER SAR, ERNESTO, „Popcorn Time“ gives users anonymity with a free built-in VPN, 7. Juni 2014, <<https://torrentfreak.com/popcorn-time-give-s-users-anonymity-with-a-free-built-in-vpn-140607/>> (besucht 25. August 2015) (zit. VAN DER SAR, Popcorn Time)
- VIANELLO, MIRKO, Abruf und Aufzeichnung von Video- und Audiostreams zum privaten Gebrauch, CR 2010, 728
- VOEGELI-WENZL, JULIA, Internet Governance am Beispiel der Internet Corporation of Assigned Names and Numbers (ICANN), GRUR-Int. 2007, 807
- VÖLTZ, GREGOR, HTML5 – neuer Standard, neue Probleme? Ein Überblick über Neuerungen und rechtliche Fragen, MMR 2013, 619

- VOLZ, STEFANIE, Trennungsgebot und Internet – Ein medienrechtliches Prinzip in Zeiten der Medienkonvergenz, Zürich 2014, zugleich: Diss. Zürich 2014
- VON ALBRECHT, MARTIN/MUTSCHLER-SIEBERT, ANNETTE/BOSCH, TOBIAS, Die Murphy-Entscheidung und ihre Auswirkungen auf Sport- und Film-lizenzen im Online-Bereich – Die exklusive territoriale Rechtevergabe ist kein Modell der Vergangenheit!, ZUM 2012, 93
- VON APPEN, JÖRG/BARATH, ALJOSHA, Nicht autorisiertes Live-Streaming von Sportereignissen, CaS 2014, 249
- VON BÜREN, ROLAND/MEER, MICHAEL A., Einleitung, in: von Büren, Roland/David Lucas (Hrsg.), SIWR II/1, 3. A., Basel 2014, 1
- VON DIEMAR, UNDINE, Die digitale Kopie zum privaten Gebrauch, Münster/Hamburg/London, zugleich: Diss. Potsdam 2002
- VON GERLACH, FELIX-TESEN, Die urheberrechtliche Bewertung des nicht-linearen Audio-Video-Streamings im Internet – die verschiedenen technischen Verfahren im System und auf dem Prüfstand urheberrechtlicher Verwertungs- und Leistungsschutzrechte, Baden-Baden 2012, zugleich: Diss. Berlin 2012
- VON UNGERN-STERMBERG, JOACHIM, Die Rechtsprechung des EUGH und des BGH zum Urheberrecht und zu den verwandten Schutzrechten im Jahre 2014, GRUR 2015, 205
- VON ZIMMERMANN, GEORG, Recording-Software für Internetradios, MMR 2007, 553
- WAND, PETER, Technische Schutzmassnahmen und Urheberrecht, München 2001, zugleich: Diss. München 2000
- WANDTKE, ARTUR-AXEL/VON GERLACH, FELIX-TESEN, Die urheberrechtliche Rechtmässigkeit der Nutzung von Audio-Video Streaminginhalten im Internet, GRUR 2013, 676
- WEBER, ROLF H., Internet-Governance – ein Überblick, digma 2014, 94 (zit. WEBER, digma 2014)
- WEBER, ROLF H., E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. A., Zürich 2010 (zit. WEBER, E-Commerce)

- WEBER, ROLF H./FERCSIK SCHNYDER, ORSOLYA, „Was für `ne Sorte von Geschöpf ist euer Krokodil?“ – Zur datenschutzrechtlichen Qualifikation von IP-Adressen, sic! 2009, 577
- WEIGELE, MARTIN, Internet Corporation on Assigned Names and Number (ICANN) – Staats-, europa- und völkerrechtliche Beurteilung, MMR 2013, 16
- WEIL, BIRGIT, Was du liebst, lass frei. Kommt es zurück, gehört es dir – für immer!, sic! 2014, 478
- WIGGER, FABIAN, AGUR12-Schlussbericht, Vorschläge zur Anpassung des Schweizer Urheberrechts an die technische Entwicklung, UFITA II/2014, 515 (zit. WIGGER, UFITA II/2014)
- WIGGER, FABIAN, EuGH: Keine Privatkopie ab unrechtmässiger Vorlage, sic! 2014, 558 (zit. WIGGER, sic! 2014)
- WIGGER, FABIAN/KORRODI, MARTIN, EuGH: Live-Streaming ab unrechtmässiger Vorlage, sic! 2013, 448
- WILD, GREGOR, Zur Konkurrenz zwischen Urheberrecht und künstlerischem Leistungsschutz, Jusletter 17. Dezember 2001
- WILLE, STEFAN, Festhalten an Vorlagefrage zum Framing, GRUR-Prax 2014, 331
- WOHLERS, WOLFGANG, „in dubio pro durior“ – zugleich Besprechung von BGer, Urteil v. 11.7.2011, 1B\_123/2011=BGE 137 IV 219, FP 2011, 370
- WULLSCHLEGER, MARC, Die Durchsetzung des Urheberrechts im Internet, Bern 2015, zugleich: Diss. Bern 2014.
- ZECH, HERBERT, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud – Das Verhältnis von Urheber- und Vertragsrecht bei Verträgen über den Werkkonsum per Cloud-Computing, ZUM 2014, 3
- ZHANG, GE/LIU, WEI/HEI, XIAOJUN/CHENG, WENQUING, Unreeling Yunlei Kankan: Understanding Hybrid CDN-P2P Video-on-demand Streaming, IEEE Transaction on Multimedia, 2015, 229
- ZINN, DANIEL, Wer sucht, der findet (nicht immer). Mit Internetzensur wird versucht den Zugriff auf rechtswidrige oder unliebsame Inhalte im Internet zu verhindern, digma 2008, 114

## Materialienverzeichnis

AGUR12, Schlussbericht AGUR12 vom 28. November 2013, abrufbar <[https://www.ige.ch/fileadmin/user\\_upload/recht/national/d/urheberrecht/Schlussbericht\\_der\\_AGUR12\\_vom\\_28\\_11\\_2013\\_DE.pdf](https://www.ige.ch/fileadmin/user_upload/recht/national/d/urheberrecht/Schlussbericht_der_AGUR12_vom_28_11_2013_DE.pdf)> (besucht 25. August 2015) (zit. AGUR12, Schlussbericht)

AGUR12 II, Medienmitteilung der Arbeitsgruppe zum Urheberrecht (AGUR12 II) vom 2. März 2017, abrufbar unter <[https://www.ige.ch/fileadmin/user\\_upload/recht/national/d/urheberrecht/AGUR12\\_II\\_Medienmitteilung\\_20170302\\_DE.pdf](https://www.ige.ch/fileadmin/user_upload/recht/national/d/urheberrecht/AGUR12_II_Medienmitteilung_20170302_DE.pdf)> (besucht 28. November 2017)

Amtliches Bulletin der Schweizerischen Bundesversammlung, Nationalrat, Bern 2007 (zit. Amtl. Bull. NR 2007)

Bericht über das Ergebnis des Vernehmlassungsverfahrens betreffend zwei Abkommen der Weltorganisation für geistiges Eigentum und Änderungen des Urheberrechtsgesetzes vom 2. Dezember 2016, abrufbar <<https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2016/2016-12-022/ve-ber-d.pdf>> (besucht 28. November 2017)

Botschaft zur Änderung des Urheberrechtsgesetzes sowie zur Genehmigung zweier Abkommen der Weltorganisation für geistiges Eigentum und zu deren Umsetzung vom 22. November 2017, BBl 2018 591 (zit. Botschaft URG 2017)

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010, BBl 2010 4697 (zit. Botschaft Cyberkriminalität)

Botschaft zum Bundesbeschluss über die Genehmigung von zwei Abkommen der Weltorganisation für geistiges Eigentum und zur Änderung des Urheberrechtsgesetzes vom 10. März 2006, BBl 2006 3389 (zit. Botschaft URG 2006)

Botschaft zum revidierten Fernmeldegesetz (FMG) vom 10. Juni 1996, BBl 1996 III 1405 (zit. Botschaft FMG 1996)

Botschaft über die Aenderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Aenderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen) vom 24. April 1991, BBl 1991 II 969 (zit. Botschaft StGB 1991)

Botschaft zu einem Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG), zu einem Bundesgesetz über den Schutz von Topographien von integrierten Schaltungen (Topographiengesetz, ToG) sowie zu einem Bundesbeschluss über verschiedene völkerrechtliche Verträge auf dem Gebiete des Urheberrechts und der verwandten Schutzrechte vom 19. Juni 1989, BBl 1989 III 477 (zit. Botschaft URG 1989)

Bundesbeschluss über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. März 2011, BBl 2011, 2767 (zit. Bundesbeschluss Cyberkriminalität)

Cisco Visual Networking Index: Forecast and Methodology, 2014-2019, 27. Mai 2015, <[http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white\\_paper\\_c11-481360.pdf](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf)> (besucht 25. August 2015)

Empfehlung des EDÖB vom 9. Januar 2008 betreffend die Bearbeitung von Personendaten im Rahmen der Bekämpfung von Urheberrechtsverletzungen in *P2P-Netzwerken*, abrufbar unter <<https://tinyurl.com/Empfehlungen-EDOEB>> (besucht 25. August 2015) (zit. Empfehlung EDÖB)

Entwurf zur Änderung des Urheberrechtsgesetzes vom 22. November 2017, BBl 2018 693 (zit. E-URG 2017)

Erläuternder Bericht zu zwei Abkommen der Weltorganisation für geistiges Eigentum und zu Änderungen des Urheberrechtsgesetzes vom 11. Dezember 2015, abrufbar unter <<https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2015/2015-12-11/vn-ber-d.pdf>> (besucht 28. November 2017) (zit. Erläuternder Bericht 2015)

IFPI, Digital Music Report 2015, <<http://www.ifpi.org/downloads/Digital-Music-Report-2015.pdf>> (besucht 25. August 2015)

NET-Metrix AG, Base 2014-1, <[http://www.net-metrix.ch/sites/default/files/files/NET-Metrix-Base/NMB\\_2014-1\\_Medienmitteilung\\_de.pdf](http://www.net-metrix.ch/sites/default/files/files/NET-Metrix-Base/NMB_2014-1_Medienmitteilung_de.pdf)> (besucht 25. August 2015).



PricewaterhouseCoopers, Global entertainment and media outlook 2015-2019 – Music, Key insights at a glance, <<http://www.pwc.com/gx/en/global-entertainment-media-outlook/assets/2015/music-key-insights-2-digital-recorded-music-revenue.pdf>> (besucht 25. August 2015)

Staatssekretariat für Wirtschaft SECO, Bericht vom 23. Januar 2014 über den Roundtable zum Urheberrecht im Internet, <<http://tinyurl.com/SECO-Roundtable-Urheberrecht>> (besucht 25. August 2015) (zit. SECO, Roundtable zum Urheberrecht)

Vorentwurf zur Änderung des Urheberrechtsgesetzes vom 11. Dezember 2015, abrufbar unter <<https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2015/2015-12-11/vorentw-urg-d.pdf>> (besucht 1. Dezember 2017) (zit. E-URG 2015)



# Einleitung

## I. Problemstellung und Zielsetzung

Der Begriff Streaming steht als Sammelbegriff für unterschiedliche technische Verfahren, mit denen digitale Inhalte über ein Netzwerk verteilt werden können.<sup>1</sup> Die Streaming-Technologie hat die Nutzung digitaler Werke nachhaltig verändert.<sup>2</sup> Begünstigt durch grössere Internetbandbreiten, Flatrates für mobiles Internet sowie durch die steigende Zahl der Internetnutzer und die Zunahme internetfähiger Endgeräte, haben sich zahlreiche neue Geschäftsmodelle herausgebildet. Mittels Streaming können Musik, Filme, Bücher und Computerspiele über das Internet verbreitet und konsumiert werden. Durch das sog. On-Demand-Streaming sind die Nutzer nicht mehr länger an fixe Programmvorgaben der Radio- oder Fernsehsender gebunden, sondern bestimmen individuell, wann sie die gewünschten Inhalte konsumieren wollen. Im Unterschied zum klassischen *Download* entfällt beim Streaming die Wartezeit, da der Datensatz nicht vorgängig vollständig auf ein Speichermedium im Nutzerrechner heruntergeladen werden muss.<sup>3</sup>

Gemäss einer Prognose des *Cisco Visual Networking Index 2014* findet bei der durchschnittlichen weltweiten Übertragungskapazität bei festen Internetverbindungen ein Anstieg von 20 Mbps im Jahre 2014 auf 43 Mbps im Jahre 2019 statt. Im gleichen Zeitraum soll der Anteil der Video-Inhalte am gesamthaft über das Internet übertragenen privaten Datenverkehr von 64 Prozent auf 80 Prozent ansteigen.<sup>4</sup> Im Jahr 2019 werden demnach jede Sekunde beinahe eine Million Minuten an Video-Inhalten über das Internet übertragen.<sup>5</sup> Schon seit geraumer Zeit ist eine stark zunehmende Verlagerung der Distribution urheberrechtlich geschützter Werke, weg vom Verkauf physi-

---

<sup>1</sup> ENSTHALER, NJW 2014, 1553; KUROSE/ROSS, 628; BRÄNDLI/TAMÒ, sic! 2013, 650; VON GERLACH, 17 f.; LONGOLIUS, 49.

<sup>2</sup> BRÄNDLI/TAMÒ, sic! 2013, 651; VON GERLACH, 11.

<sup>3</sup> Vgl. Rz. 12 ff.

<sup>4</sup> Noch nicht miteingerechnet in dieser Prozentzahl sind Video-Inhalte, die über *P2P-Filesharing-Netzwerke* übertragen werden.

<sup>5</sup> Vgl. zum Ganzen <[http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white\\_paper\\_c11-481360.pdf](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.pdf)> (besucht 25. August 2015).

scher Datenträger, hin zum Streaming zu beobachten.<sup>6</sup> Laut der Internetstudie *NET-Matrix-Base* nutzten im Jahr 2014 rund 3,8 Millionen Einwohner in der Schweiz regelmässig Streaming-Angebote.<sup>7</sup> Zuzufolge einer repräsentativen Umfrage des *BITKOM* ersetzen in Deutschland rund ein Drittel der Nutzer ab 14 Jahren das klassische Fernsehen ganz oder teilweise durch Streaming-Angebote.<sup>8</sup> Nach dem *Digital Music Report 2015* des IFPI liegen die Einnahmen aus dem digitalen Geschäft mit Musik erstmals gleichauf mit jenen aus dem physischen Geschäft.<sup>9</sup>

- 3 Neben zahlreichen neuen Verwertungs- und Distributionsmöglichkeiten, welche sich durch die Streaming-Technologie für die Urheber und Rechteinhaber eröffnen, ergeben sich auch neue Risiken. So können etwa urheberrechtlich geschützte Werke ohne Einwilligung der Rechteinhaber auf Server hochgeladen und über das Internet mittels Streaming-Verfahren öffentlich zugänglich gemacht werden. Sodann ermöglicht das sog. *P2P-Streaming*, dass urheberrechtlich geschützte Werke direkt zwischen den am Netzwerk beteiligten Nutzern ausgetauscht werden können (*Filesharing*).
- 4 Ziel der vorliegenden Arbeit ist es, das Streaming von urheberrechtlich geschützten Werken aus (urheber-)strafrechtlicher Perspektive zu beleuchten. Anhand ausgewählter Fallbeispiele soll aufgezeigt werden, wo beim Streaming die Grenze zwischen einer legalen Werkverwendung und einer Urheberrechtsverletzung liegt.

## II. Gang der Untersuchung

- 5 Im ersten Teil der Arbeit folgen eine Darstellung der technischen Grundlagen der verschiedenen Streaming-Verfahren sowie eine kurze Übersicht über die rechtlichen Grundlagen des Schweizer Urheberrechts.

---

<sup>6</sup> Für die Musikbranche vgl. etwa <<http://www.pwc.com/gx/en/global-entertainment-media-outlook/assets/2015/music-key-insights-2-digital-recorded-music-revenue.pdf>> (besucht 25. August 2015).

<sup>7</sup> NET-Matrix AG, Base 2014-1, <[http://www.net-matrix.ch/sites/default/files/files/NET-Matrix-Base/NMB\\_2014-1\\_Medienmitteilung\\_de.pdf](http://www.net-matrix.ch/sites/default/files/files/NET-Matrix-Base/NMB_2014-1_Medienmitteilung_de.pdf)> (besucht 25. August 2015).

<sup>8</sup> KUNTZ, MMR-Aktuell 2014, 363971; <[https://www.bitkom.org/Presse/Presseinformation/Pressemitteilung\\_5191.html](https://www.bitkom.org/Presse/Presseinformation/Pressemitteilung_5191.html)> (besucht 25. August 2015).

<sup>9</sup> <<http://www.ifpi.org/downloads/Digital-Music-Report-2015.pdf>> (besucht 25. August 2015).

Der zweite Teil ist der rechtlichen Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus der Perspektive des Stream-Anbieters gewidmet. Hierbei wird untersucht, welche Rechte bei den verschiedenen Streaming-Verfahren tangiert sind. Ebenso wird eine rechtliche Bewertung des *Framing* vorgenommen. Neben einer Vielzahl legaler Streaming-Dienste, existieren auch einige populäre illegale Streaming-Webseiten, auf denen – ohne die Einwilligung der Rechteinhaber – urheberrechtlich geschützte Werke öffentlich zugänglich gemacht werden. Ausgehend vom Fallbeispiel der mittlerweile geschlossenen illegalen Streaming-Webseite *kino.to*, deren Geschäftsmodell aufgrund zahlreicher Nachfolgeseiten noch immer aktuell ist, wird eine Bewertung sämtlicher an dieser Organisation beteiligter Personen, aus Sicht des Schweizer Urheber- und Strafrechts, vorgenommen. 6

Die Rollenverteilung zwischen Anbietern und Nutzern tritt zunehmend in den Hintergrund.<sup>10</sup> Zahlreiche Streaming-Portale ermöglichen es ihren Nutzern, digitale Inhalte kostenlos hochzuladen und anderen Nutzern als Stream zugänglich zu machen.<sup>11</sup> Durch die Verwendung sog. *Live-Streaming-Apps* können Nutzer beliebige Inhalte live und in Echtzeit über das Internet verbreiten. Soweit es sich bei den öffentlich zugänglich gemachten Inhalten um urheberrechtlich geschützte Werke handelt, ist die Einhaltung des Urheberrechts zu überprüfen. 7

Der dritte Teil der Arbeit befasst sich mit der rechtlichen Bewertung des Streaming geschützter Werke aus Sicht des Nutzers. Dabei wird vorab die zentrale Frage geklärt, ob die im Rahmen des Streaming im Nutzerrechner hergestellten Zwischenspeicherungen als urheberrechtlich relevante Werknutzung oder als urheberrechtsfreier rezeptiver Werkgenuss zu qualifizieren sind. Im Zusammenhang mit der Nutzung nicht-lizenzierter Streaming-Angebote muss sodann geprüft werden, ob sich die Nutzer auf die Schrankenregelungen des Urheberrechts berufen können. Das Augenmerk richtet sich dabei primär auf die Schranke für technisch bedingte Vervielfältigungen ohne eigenständige wirtschaftliche Bedeutung gem. Art. 24a URG. Soweit die Nutzungshandlungen innerhalb des Privatgebrauchs stattfinden, wird zudem eine Subsumtion unter die Schrankenregelung zugunsten des Privatgebrauchs nach Art. 19 Abs. 1 lit. a URG geprüft. Anschliessend werden 8

---

<sup>10</sup> So auch VON GERLACH, 13.

<sup>11</sup> Man spricht dabei von user-generated-content (UGC); vgl. dazu auch REINEMANN/REMMERTZ, ZUM 2012, 216 ff.

verschiedene Möglichkeiten aufgezeigt, wie die Verwertung digitaler Werke mittels Streaming, durch den Einsatz technischer Massnahmen, gegen urheberrechtswidrige Handlungen geschützt werden kann. Dabei liegt der Fokus auf den rechtlichen Bestimmungen zum Schutze technischer Massnahmen. Anhand von Fallbeispielen werden die Sanktionsmöglichkeiten nach Schweizer Urheber- und Strafrecht aufgezeigt, mit denen die Umgehung von Zugangs- und Nutzungsschranken sowie allfällige Tathandlungen im Vorfeld der eigentlichen Umgehungshandlung bestraft werden können.

- 9 Im vierten Teil findet eine rechtliche Bewertung des *P2P-Streaming* statt. Bei diesem Streaming-Verfahren werden die Daten nicht von einem zentralen Server geladen, sondern dezentral über das sog. *BitTorrent*-Protokoll zwischen den am Netzwerk beteiligten Nutzern ausgetauscht. Nebst der urheberstrafrechtlichen Verantwortlichkeit der am *P2P-Streaming* beteiligten Nutzer wird sodann auch die Strafbarkeit der übrigen Beteiligten untersucht.
- 10 Der fünfte Teil der Arbeit setzt sich mit den praktischen Schwierigkeiten bei der Rechtsdurchsetzung auseinander, die bei Urheberrechtsverletzungen im Rahmen des Streaming auftreten. Die Strafverfolgung bei Internetdelikten wird dadurch erschwert, dass die Täter aufgrund der Globalität des Internets regelmässig weitgehend anonym oder aus Ländern heraus agieren, in denen Urheberrechtsverletzungen nicht oder nicht effektiv geahndet werden. Vorab werden deshalb die Probleme *de lege lata* bei der Datenbearbeitung zur Identitätsermittlung von Urheberrechtsverletzern im Internet analysiert. Sodann wird ein Regelungsvorschlag zur Änderung des DSG präsentiert, der eine rechtskonforme Identitätsermittlung von Urheberrechtsverletzern anhand von deren Internetverbindungsdaten ermöglichen soll. Unter Berücksichtigung der Vorschläge der AGUR12<sup>12</sup> zur besseren Durchsetzung von Urheberrechten im digitalen Umfeld wird abgeklärt, ob ein etwaiger Anpassungsbedarf des geltenden Rechts besteht, damit Urheberrechtsverletzungen im Internet wirksam verfolgt und geahndet werden können.
- 11 Die Untersuchung endet mit einer Zusammenfassung der wesentlichen Ergebnisse dieser Arbeit. In einem kurzen Nachtrag werden abschliessend noch die wichtigsten Entwicklungen in der Urheberrechtsrevision aufgezeigt, die seit Abgabe und vor Drucklegung dieser Arbeit eingetreten sind.

---

<sup>12</sup> Vgl. <<https://www.ige.ch/urheberrecht/agur12.html>> (besucht 25. August 2015).

# 1. Teil: Technische und rechtliche Grundlagen des Streaming

## I. Technische Einführung

### 1. Streaming von Audio-/Video-Dateien

Der Begriff Audio-/Video-Streaming steht für das gleichzeitige Empfangen und Wiedergeben von Audio- und/oder Videodaten aus dem Rechnernetz.<sup>13</sup> Die Streaming-Technologie basiert auf einer Echtzeitkommunikation zwischen *Server* und *Client*, weshalb stets eine bestehende Internetverbindung vorausgesetzt ist.<sup>14</sup> Gegenüber dem klassischen Download bietet das Streaming den Vorteil, dass die digitalen Inhalte vor ihrer Nutzung nicht zunächst vollständig auf ein Speichermedium kopiert werden müssen.<sup>15</sup> Der Abspielvorgang der Datei beginnt beinahe zeitgleich mit dem Abruf des Inhalts.<sup>16</sup> Im Unterschied zum klassischen Download werden die Inhalte beim Streaming i.d.R. nicht dauerhaft auf einem Speichermedium im Nutzerrechner abgespeichert.<sup>17</sup>

---

<sup>13</sup> HILGERT/GRETH, 103, verstehen darunter eine Technik, „die kontinuierliche Datenströme zwischen Rechnern eines Netzes, zum Beispiel im Internet, ermöglicht“; GALETZKA/STAMER, MMR 2014, 292, sprechen beim „Streaming“ von einem Oberbegriff für Streaming Audio und Streaming Video; HEINEMEYER/KREITLOW, MMR 2013, 624, m.w.H.; STOLZ, MMR 2013, 353, mit dem Hinweis, dass der Begriff „Streaming“ bloss den Vorgang der Übertragung von Daten bezeichnet. Mit Blick auf die Inhalte spricht man indessen von „Streaming-Media“; EICHELBERGER, 19; SCHÄUFELE, 33; STIEPER, MMR 2012, 12; VON GERLACH, 47; LONGOLIUS, 43; BUSCH, GRUR 2011, 496 f.; FANGEROW/SCHULZ, GRUR 2010, 678; GLARNER, Musikpiraterie im Internet, 120 f.; BÜHLER, 200.

<sup>14</sup> HILGERT/GRETH, 82; LONGOLIUS, 49.

<sup>15</sup> SCHEDER-BIESCHIN, 165; HEINEMEYER/KREITLOW, MMR 2013, 624; BRÄNDLI/TAMÒ, sic! 2013, 652; EICHELBERGER, 19; BUSCH, GRUR 2011, 496; FANGEROW/SCHULZ, GRUR 2010, 677 f.; KOCH, GRUR 2010, 574; BÜSCHER/MÜLLER, GRUR 2009, 558.

<sup>16</sup> EICHELBERGER, 19; KOCH, GRUR 2010, 574; HEINEMEYER/KREITLOW, MMR 2013, 624.

<sup>17</sup> BRÄNDLI/TAMÒ, sic! 2013, 653; BUSCH, GRUR 2011, 497; LONGOLIUS, 50.

- 13 Zur Datenübertragung im Internet werden zwei unterschiedliche Streaming-Protokolle eingesetzt: Entweder wird das *Transmission Control Protocol (TCP)* oder das *User Datagram Protocol (UDP)* verwendet.<sup>18</sup> Im Unterschied zum *TCP* ist das *UDP* ein verbindungsloses, unzuverlässiges Protokoll für die Abwicklung der Datenübertragung, da es keinen Rückkanal hat, der Datenlieferungen quittiert.<sup>19</sup> Beim *UDP* kann es daher zu Paketverlusten kommen. Dafür arbeitet das *UDP* schneller als das *TCP*.<sup>20</sup>
- 14 Die Audio- und Videodateien der Streaming-Plattformen werden vornehmlich als *Flash* angeboten, zu deren Wiedergabe überwiegend der *Adobe Flash Player*<sup>21</sup> als *Browser Plug-In* verwendet wird.<sup>22</sup> Seit einiger Zeit werden Videoclips vermehrt auch in einem anderen Format per *HTML5* direkt in die Webseite eingebunden, da so ausser dem *Browser*<sup>23</sup> keine zusätzliche Software installiert werden muss.<sup>24</sup>
- 15 Während beim *Filesharing* der Austausch und das Speichern der Daten im Vordergrund stehen, zielt das Streaming primär auf den reinen Werkgenuss ab.<sup>25</sup> Eine Zwischenspeicherung auf dem Endgerät des Nutzers findet, technisch bedingt, trotzdem statt, weil die empfangenen Daten zur Verarbeitung zumindest vorübergehend zwischengespeichert werden müssen.<sup>26</sup> Um Schwankungen der Bandbreiten bei der Datenübertragung zwischen dem *Server* und dem *Browser* des Endgeräts auszugleichen, werden kontinuier-

---

<sup>18</sup> SCHREINER, 109 ff.; KUROSE/ROSS, 628 ff., die zwischen *UDP*-Streaming, *HTTP*-Streaming und adaptivem *HTTP*-Streaming differenzieren; WANDTKE/VON GERLACH, GRUR 2013, 677; VON GERLACH, 39 ff.; HEID, 15; BRÄNDLI/TAMÒ, sic! 2013, 653; BUSCH, GRUR 2011, 497 f.; LONGOLIUS, 51 ff.

<sup>19</sup> KUROSE/ROSS, 223 ff.; VON GERLACH, 43; BRÄNDLI/TAMÒ, sic! 2013, 653.

<sup>20</sup> KUROSE/ROSS, 223 ff.; VON GERLACH, 43 ff.; WANDTKE/VON GERLACH, GRUR 2013, 677.

<sup>21</sup> BRUNOTTE, 15 f.; <<http://get.adobe.com/de/flashplayer>> (besucht 25. August 2015).

<sup>22</sup> JANISCH/LACHENMANN, MMR 2013, 213; andere verbreitete Player sind QuickTime von Apple, der Windows Media Player von Microsoft oder der VLC Mediaplayer.

<sup>23</sup> z.B. Internet Explorer, Mozilla Firefox, Google Chrome oder Safari von Apple.

<sup>24</sup> Ausführlich dazu VÖLTZ, MMR 2013, 619 ff.; JANISCH/LACHENMANN, MMR 2013, 213; <<https://www.youtube.com/html5?hl=de>> (besucht 25. August 2015).

<sup>25</sup> HILGERT/HILGERT, MMR 2014, 86.

<sup>26</sup> HILGERT/HILGERT, MMR 2014, 86; WANDTKE/VON GERLACH, GRUR 2013, 677, mit detaillierten Ausführungen zum Umfang der Zwischenspeicherung; BÄCKER/HÖFINGER, ZUM 2013, 624; FANGEROW/SCHULZ, GRUR 2010, 677; RADMANN, ZUM 2010, 388; FANGEROW/SCHULZ, GRUR 2010, 678.



lich Daten gepuffert, um eine reibungslose Wiedergabe der Audio-/Video-Datei zu gewährleisten.<sup>27</sup> Eine dauerhafte Speicherung der Daten findet gewöhnlich nicht statt. Im Regelfall werden die Daten nur temporär gespeichert und fortlaufend überschrieben oder spätestens mit dem Schliessen des *Browsers* oder dem Herunterfahren des Computers gelöscht.<sup>28</sup> Bereits an dieser Stelle sei erwähnt, dass es für technisch versierte Nutzer sowie durch den Einsatz bestimmter Programme auch beim Streaming möglich ist, dauerhafte Kopien von gestreamten Inhalten herzustellen.<sup>29</sup>

Beim Streaming können als Wiedergabegeräte etwa Computer, Notebooks, 16  
Tablet-PCs, Mobiltelefone (internetfähige „Smartphones“), Spielekonsolen, internetfähige Fernsehgeräte („Smart-TVs“) oder Internet-Radiogeräte eingesetzt werden.<sup>30</sup> Bei der Streaming-Technologie kann grundsätzlich zwischen zwei verschiedenen Kategorien differenziert werden: das lineare *Live-Streaming* und das nicht-lineare *On-Demand-Streaming*.<sup>31</sup> Der Hauptunterschied zwischen den beiden Streaming-Kategorien liegt darin, dass je nach Kategorie der Anbieter oder der Nutzer über den Zeitpunkt der Übertragung der Inhalte bestimmt.<sup>32</sup> Während beim Live-Streaming der Zeitpunkt der Wiedergabe durch den Anbieter festgelegt wird, kann beim On-Demand-Streaming der Nutzer selbst den Zeitpunkt des Abspielvorgangs steuern.<sup>33</sup>

Gewisse Autoren unterscheiden noch eine dritte Kategorie, das sog. Near- 17  
on-Demand-Streaming.<sup>34</sup> Da der Nutzer auch beim Near-on-Demand-

<sup>27</sup> HILGERT/GRETH, 103; BÄCKER/HÖFINGER, ZUM 2013, 624; RADMANN, ZUM 2010, 388; FANGEROW/SCHULZ, GRUR 2010, 678.

<sup>28</sup> HILGERT/HILGERT, MMR 2014, 86; STOLZ, MMR 2013, 354; FANGEROW/SCHULZ, GRUR 2010, 678; RADMANN, ZUM 2010, 388.

<sup>29</sup> HILGERT/GRETH, 104; BUSCH, GRUR 2011, 497; RADMANN, ZUM 2010, 388, m.w.H.

<sup>30</sup> VON GERLACH, 11; KOCH, GRUR 2010, 574.

<sup>31</sup> HILGERT/GRETH, 104 f. und GALETZKA/STAMER, MMR 2014, 292, differenzieren zwischen Live-Streaming und On-Demand-Streaming; VON GERLACH, 47; EICHELBERGER, 20; OĞLAKCIOĞLU, ZIS 2012, 433; STIEPER, MMR 2012, 12 f.; KOCH, GRUR 2010, 574.

<sup>32</sup> HILGERT/GRETH, 104; EICHELBERGER, 20; VON GERLACH, 50 ff.

<sup>33</sup> BRÄNDLI/TAMÒ, sic! 2013, 656; VON GERLACH, 50 ff.

<sup>34</sup> PRILL, 18 f., die auch von sog. „Loop-Streams“ spricht; VON GERLACH, 47, 52.

Streaming an einen festen Sendeplan gebunden ist, handelt es sich dabei um eine Variante des linearen Streamings.<sup>35</sup>

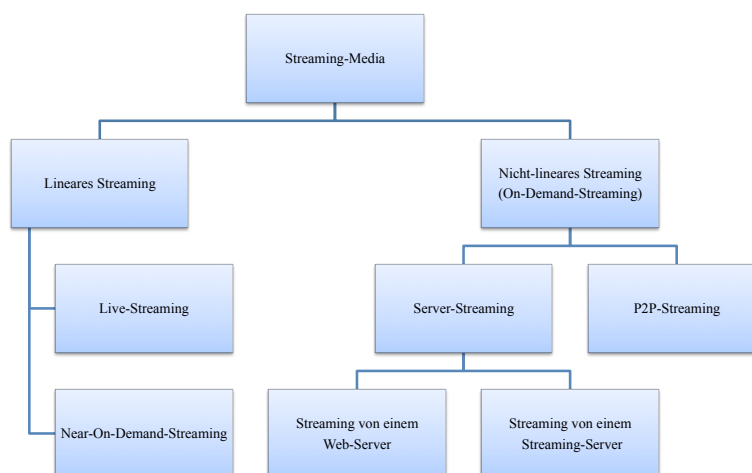


Abbildung 1: Übersicht über die verschiedenen Streaming-Verfahren

## A. Lineares Streaming

### a) Live-Streaming

- 18 Beim Live-Streaming bestimmt der Anbieter den Anfangszeitpunkt der Übertragung.<sup>36</sup> Gewöhnlich handelt es sich dabei um ein *serverbasiertes* Streaming, bei welchem die Mediendatei von einem zentralen *Server* auf die Rechner der Nutzer übertragen wird.<sup>37</sup> Der Datenstrom wird in Echtzeit komprimiert, encodiert, mit Kopierkontroll- sowie Steuerinformationen und Zeitstempeln („time stamps“) versehen und in formatierten, kleinen Datenpaketen sequenziell von einem *Serverrechner* an alle Empfangsgeräte („one-to-many“) im Multicast-Verfahren<sup>38</sup> übertragen und decodiert.<sup>39</sup> Die Interak-

---

<sup>35</sup> Vgl. BRÄNDLI/TAMÖ, sic! 2013, 656 m.w.H.; VON GERLACH, 52.

<sup>36</sup> HILGERT/GRETH, 104; BRÄNDLI/TAMÖ, sic! 2013, 655 f.; EISELE, 224; VON GERLACH, 50.

<sup>37</sup> VON APPEN/BARATH, CaS 2014, 250; STOLZ, MMR 2013, 354.

<sup>38</sup> GALETZKA/STAMER, MMR 2014, 292, umschreiben die Bezeichnung Multicast als einen Vorgang, bei dem die Daten zeitgleich von einem Punkt an eine Gruppe mit beliebig vielen Empfängern zu einer bestimmten Zeit übertragen wird; LONGOLIUS, 28.

tionsmöglichkeiten der Nutzer sind auf die Teilnahme am laufenden Programm beschränkt, ein Vor- oder Zurückspulen des Werks ist nicht möglich.<sup>40</sup> Im Unterschied zum On-Demand-Streaming existiert die zu übertragende Datei zu Beginn der Übertragung noch nicht auf einem *Server*.<sup>41</sup> Jedoch werden auch beim Live-Streaming – technisch bedingt – während der Übertragung jeweils einige Sekunden umfassende Fragmente des Werks auf dem *Server* zwischengespeichert und sodann nach Gebrauch entweder automatisch wieder gelöscht oder von der nächsten Sequenz überschrieben.<sup>42</sup> Beim Empfänger sind ephemere Zwischenspeicherungen der übertragenen Daten im *Client-Puffer* notwendig, um technisch bedingte Schwankungen bei der Übertragung auszugleichen.<sup>43</sup>

### **b) Near-on-Demand-Streaming**

Charakteristisch für das Near-on-Demand-Streaming ist, dass der Anbieter gewisse Intervalle festlegt, in denen die Inhalte beginnen (Wiederholungsschleifen).<sup>44</sup> Die Nutzer selbst können darauf keinen direkten Einfluss nehmen, sondern einzig zwischen den vom Stream-Anbieter fest vorgegebenen Startzeitpunkten auswählen.<sup>45</sup>

## **B. Nicht lineares Streaming (On-Demand-Streaming)**

Beim nicht linearen On-Demand-Streaming wird die Datenübertragung orts- und zeitunabhängig durch den individuellen Abruf des Nutzers ausgelöst.<sup>46</sup> Der Nutzer erhält vom Stream-Anbieter einen grundsätzlich nur für ihn bestimmten und allein von ihm empfangbaren Stream zur Verfügung gestellt

<sup>39</sup> VON APPEN/BARATH, CaS 2014, 250; GALETZKA/STAMER, MMR 2014, 292; VON GERLACH, 51; STIEPER, MMR 2012, 13; KOCH, GRUR 2010, 574.

<sup>40</sup> RADMANN, ZUM 2010, 388; EICHELBERGER, 20.

<sup>41</sup> STIEPER, MMR 2012, 13.

<sup>42</sup> VON APPEN/BARATH, CaS 2014, 250; STOLZ, MMR 2013, 354; STIEPER, MMR 2012, 13.

<sup>43</sup> VON APPEN/BARATH, CaS 2014, 251; STOLZ, MMR 2013, 354; STIEPER, MMR 2012, 12; BUSCH, GRUR 2011, 497 f.; RADMANN, ZUM 2010, 388.

<sup>44</sup> EISELE, 223; EICHELBERGER, 22; VON GERLACH, 52; JOLLER, 14 f.

<sup>45</sup> EICHELBERGER, 22.

<sup>46</sup> WANDTKE/VON GERLACH, GRUR 2013, 676; STOLZ, MMR 2013, 354; JOLLER, 14; BÜSCHER/MÜLLER, GRUR 2009, 558.

(Unicast).<sup>47</sup> Ein Vor- und Zurückspulen oder Pausieren während der Wiedergabe ist ebenfalls möglich.<sup>48</sup> Die vom Nutzer angeforderten digitalen Inhalte werden paketweise übertragen, beim Empfänger durch spezielle Software (Client)<sup>49</sup> decodiert und in einem Puffer (Cache) im RAM oder auf der Festplatte des Zielrechners zwischengespeichert.<sup>50</sup> Die Zwischenspeicherung („Zwischenpufferung“) von Dateiteilen ist erforderlich, um trotz variabler Übertragungsraten und unterschiedlicher Laufzeiten der Datenpakete (Jitter<sup>51</sup>) eine verzögerungsfreie Wiedergabe der empfangenen Daten zu gewährleisten.<sup>52</sup> Die Wiedergabe startet deshalb nicht unmittelbar mit dem Beginn der Datenübertragung, weil vorab die ersten Sekunden der Video- oder Audiodatei zwischengespeichert werden.<sup>53</sup>

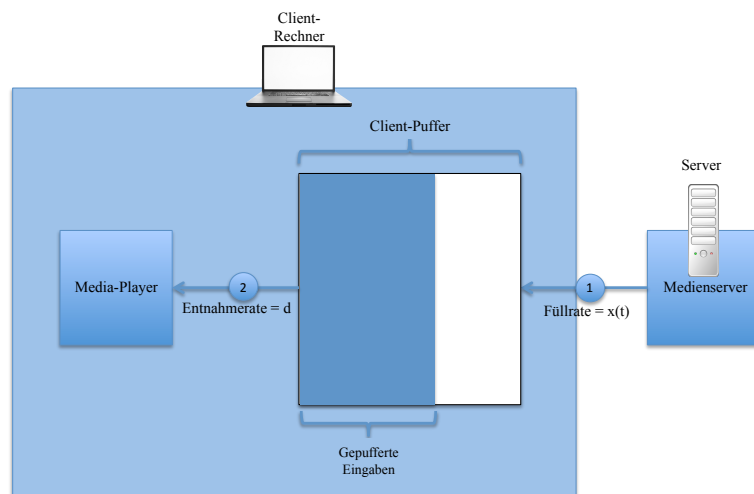


Abbildung 2: Client-Puffer wird mit Eingaben von Medienserver mit der Rate  $x(t)$  gefüllt und wird mit der Rate  $d$  geleert, Quellen: KUROSE/ROSS, 633; TANENBAUM/WETHERALL, 814.

---

<sup>47</sup> EICHELBERGER, 21; WANDTKE/VON GERLACH, GRUR 2013, 676; STOLZ, MMR 2013, 354.

<sup>48</sup> GALETZKA/STAMER, MMR 2014, 292; STIEPER, MMR 2012, 12, BÜSCHER/MÜLLER, GRUR 2009, 558.

<sup>49</sup> z.B. der *Flash Player* von *Adobe*, *Quicktime* von *Apple* oder der *Windows Media Player* von *Microsoft*.

<sup>50</sup> STIEPER, MMR 2012, 13; RADMANN, ZUM 2010, 388; KOCH, GRUR 2010, 574 f.

<sup>51</sup> KUROSE/ROSS, 650; TANENBAUM/WETHERALL, 467 und 625 ff.

<sup>52</sup> Ausführlich zu technischen Abläufen: EISELE, 223; vgl. auch STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 496 f.; KOCH, GRUR 2010, 574 f.

<sup>53</sup> RADMANN, ZUM 2010, 387 f.

**a) Verschiedene Arten des On-Demand-Streaming**

Beim On-Demand-Streaming wird weiter differenziert zwischen dem sog. *True-On-Demand-Streaming*, dem *Progressive Download* und dem *Progressive Download* mit *http-Pseudo-Streaming*.<sup>54</sup> 21

**aa) True-On-Demand-Streaming**

Beim *True-On-Demand-Streaming* erfolgt keine Abspeicherung einer kompletten, eigenständig nutzbaren Werkkopie auf dem Zielrechner.<sup>55</sup> Es werden lediglich – abhängig von der eingestellten Puffergrösse – einzelne Segmente im Zwischenspeicher abgelegt, die wieder überschrieben werden, sobald das Abspielprogramm die Daten ausgelesen hat.<sup>56</sup> Mit gewissen Programmen ist es zwar technisch möglich, den Puffer so einzurichten, dass die gesamte Datei gepuffert wird, standardmässig werden allerdings nur wenige Sekunden zwischengespeichert.<sup>57</sup> 22

**bb) Progressive Download**

Falls die ankommenden Datenpakete auf der Festplatte des Nutzerrechners<sup>58</sup> 23 dauerhaft und zusammengesetzt abgespeichert werden, sodass am Ende der Übertragung eine vollständige Kopie auf dem Nutzerrechner vorliegt, spricht man nicht mehr von „echtem“ On-Demand-Streaming (*True-On-Demand-Streaming*), sondern von einem *Progressive Download*.<sup>59</sup> Ebenso wie beim klassischen Download wird auch beim *Progressive Download* eine vollständige Werkkopie hergestellt.<sup>60</sup> Der *Progressive Download*, bei dem typischerweise das http-Protokoll verwendet wird, ist eine Weiterentwicklung des klassischen Downloadverfahrens.<sup>61</sup> Die Speicherung erfolgt entweder im

---

<sup>54</sup> GALETZKA/STAMER, MMR 2014, 293; LONGOLIUS, 44 ff.

<sup>55</sup> GALETZKA/STAMER, MMR 2014, 293; JANISCH/LACHENMANN, MMR 2013, 213; STIEPER, MMR 2012, 13; KOCH, GRUR 2010, 574.

<sup>56</sup> STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 496.

<sup>57</sup> JANISCH/LACHENMANN, MMR 2013, 213; STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 496 f.

<sup>58</sup> Etwa im „temp“-Speicher; vgl. KOCH, GRUR 2010, 575.

<sup>59</sup> GALETZKA/STAMER, MMR 2014, 293; STIEPER, MMR 2012, 13; EICHELBERGER, 22; BUSCH, GRUR 2011, 496 ff.; KOCH, GRUR 2010, 574 f.; LONGOLIUS, 49 f.

<sup>60</sup> EICHELBERGER, 22.

<sup>61</sup> LONGOLIUS, 44.

Arbeitsspeicher oder auf der Festplatte des Nutzerrechners.<sup>62</sup> Ob die Vervielfältigung dauerhaft erfolgt oder die Datei nach dem Filmabschnitt oder jedenfalls mit dem Herunterfahren des Rechners gelöscht wird, hängt von der eingesetzten Software sowie den jeweiligen Einstellungen ab.<sup>63</sup>

cc) *Progressive Download mit http-Pseudo-Streaming*

- 24 Derweil der Nutzer im klassischen Progressive-Download-Verfahren nur innerhalb der bereits heruntergeladenen Audio-/Video-Datei hin- und herspringen kann, ermöglicht das sog. „http-Pseudo-Streaming“, an eine beliebige Stelle innerhalb der Mediendatei zu springen.<sup>64</sup> Ebenso wie beim *Progressive Download* wird auch bei diesem Vorgang eine Werkkopie auf der Festplatte des Endgeräts angefertigt.<sup>65</sup> Die Übertragung von Livesignalen ist auch hier ausgeschlossen, da diese Technologie nur bei zuvor produzierten Audio-/Video-Dateien im On-Demand-Verfahren angewendet werden kann.<sup>66</sup>

b) ***Technische Umsetzung der Distribution der Inhalte beim On-Demand-Streaming***

- 25 Beim On-Demand-Streaming wird mit Blick auf die Verteilung der Inhalte zwischen dem Server-Streaming und dem Peer-to-Peer Streaming (auch *P2P-Streaming* genannt) unterschieden.<sup>67</sup> Beim *P2P-Streaming* erfolgt die Distribution der Daten durch die Nutzer selbst, während das *Server-Streaming* dadurch gekennzeichnet ist, dass die Daten von einem zentralen Server an die einzelnen Nutzerrechner weiterverbreitet werden.<sup>68</sup> Sodann wird beim *Server-Streaming* differenziert zwischen dem Streaming von einem *Web-Server* und dem Streaming von einem *Streaming-Server*.<sup>69</sup>

---

<sup>62</sup> GALETZKA/STAMER, MMR 2014, 293; EISELE, 223 f.; LONGOLIUS, 44 ff.

<sup>63</sup> GALETZKA/STAMER, MMR 2014, 293; SOLMECKE, CR 2014, 137, der den Begriff „progressives Streaming“ verwendet; REDLICH, K&R 2014, 73; STIEPER, MMR 2012, 13.

<sup>64</sup> LONGOLIUS, 47 ff.

<sup>65</sup> STOLZ, MMR 2013, 354; JANISCH/LACHENMANN, MMR 2013, 213; LONGOLIUS, 48; KOCH, GRUR 2010, 575; MITSCHKE/ROTH, MMR 2009, 731.

<sup>66</sup> KUROSE/ROSS, 628 f.; LONGOLIUS, 48.

<sup>67</sup> VON GERLACH, 53; TANENBAUM/WETHERALL, 808 ff.

<sup>68</sup> VON GERLACH, 53.

<sup>69</sup> VON GERLACH, 53 ff.

## aa) Streaming von einem Web-Server

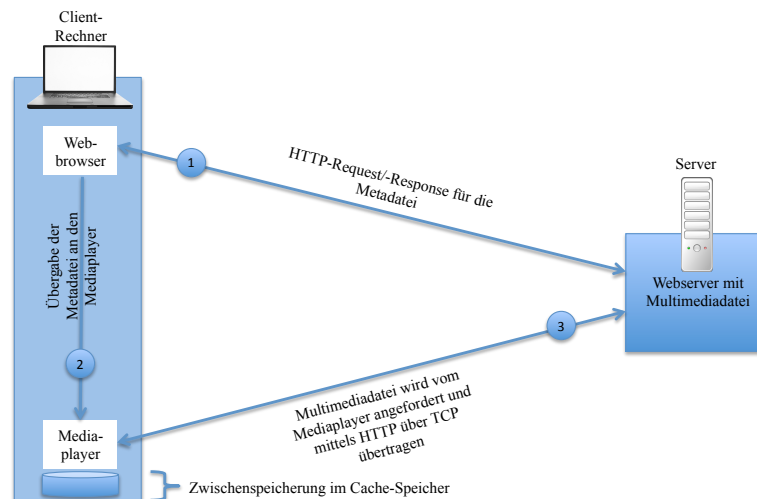


Abbildung 3: Streaming von einem Webserver auf einen Media-Player, Quelle: VON GERLACH, 55 f.

Beim Streaming von einem *Web-Server* wird die Audio-/Video-Datei vom Nutzer über den *Web-Browser* abgerufen (*HTTP-Request*). Anschliessend werden vom *Web-Server* eine oder mehrere (*Pseudo-Streaming*) computer-generierte Metadatei(en) in einer *HTTP-Response-Nachricht* an den *Client-Browser* gesendet. Der *Client-Browser* untersucht die *Response-Nachricht*, startet den zugehörigen *Media-Player* und übermittelt diesem die Metadaten. Gestützt auf die Informationen aus der Metadatei kann der *Media-Player* den Stream vom Webserver anfordern. Beim Streaming von einem *Webserver* erfolgt die Übertragung der Daten mittels *HTTP* wobei als Transportschicht das *TCP* verwendet wird.<sup>70</sup>

Am Ende der Wiedergabe befindet sich im *Cache-Speicher* des Nutzerrechners eine komplette Zwischenspeicherung der Audio-/Video-Datei. Wurde während der Wiedergabe innerhalb der Audio-/Video-Datei vorgespult, liegt eine vollständige Zwischenspeicherung ab dem vorgespulten Zeitpunkt vor (*Pseudo-Streaming*).<sup>71</sup>

<sup>70</sup> Vgl. zum Ganzen KUROSE/ROSS, 647 f.; VON GERLACH, 81 f.; LONGOLIUS, 49 ff.

<sup>71</sup> VON GERLACH, 55 f. und 81 f., weist darauf hin, dass diese Zwischenspeicherung auf verschiedene Art und Weise dauerhaft auf der Festplatte des Nutzers abgespeichert werden kann.

bb) *Streaming von einem Streaming-Server*

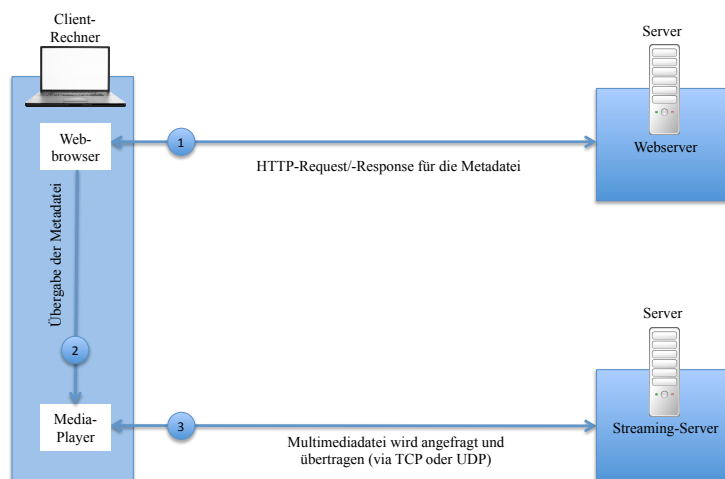


Abbildung 4: Streaming von einem Streaming-Server auf einen Media-Player, Quellen: VON GERLACH, 62 ff.; TANENBAUM/WETHERALL, 810.

- 28 *Streaming-Server* ermöglichen die Übertragung von Audio-/Video-Dateien über *HTTP/TCP* sowie alternativ über *UDP*.<sup>72</sup> Im Unterschied zum Streaming von einem *Web-Server* werden beim Streaming von einem *Streaming-Server* zwei verschiedene *Server* benötigt.<sup>73</sup> Der erste *Server* (*Web-Server*) verwaltet die Webseiten, während der zweite *Server* (*Streaming-Server*) die Multimediale Inhalte bereithält.<sup>74</sup> Der *Media-Player* fordert die Datei direkt und unter Verwendung eigener Protokolle beim *Streaming-Server* an.<sup>75</sup> Die Übertragung der Dateien erfolgt entweder verschlüsselt oder unverschlüsselt.<sup>76</sup> Als Verschlüsselungstechniken kann bspw. eine *TLS-Paketverschlüsselung*<sup>77</sup> oder ein proprietäres Verfahren (z.B. *RTMPE*) eingesetzt werden.<sup>78</sup> Die vom *Streaming-Server* ausgelieferten Datensegmente werden aufgrund der Echtzeitkommunikation umgehend nach ihrer Wiedergabe durch den *Media-Player* vernichtet. Im Gegensatz zum Streaming ab einem *Web-Server* findet beim

<sup>72</sup> KUROSE/ROSS, 647; TANENBAUM/WETHERALL, 810 f.

<sup>73</sup> TANENBAUM/WETHERALL, 810 f.; KUROSE/ROSS, 647 f.

<sup>74</sup> KUROSE/ROSS, 648.

<sup>75</sup> KUROSE/ROSS, 647 f.; VON GERLACH, 82 f.

<sup>76</sup> LONGOLIUS, 51.

<sup>77</sup> SCHREINER, 144.

<sup>78</sup> HEINEMEYER/KREITLOW, MMR 2013, 625 f.; LONGOLIUS, 51.



Streaming von einem Streaming-Server keine Zwischenspeicherung im Cache-Speicher des Nutzers statt.<sup>79</sup>

### C. P2P-Streaming

Im Gegensatz zum *Server-Streaming*, bei dem die Daten über einen zentralen Server an die Nutzer verteilt werden, erfolgt die Distribution der Daten beim *P2P-Streaming* direkt zwischen den Nutzern selbst.<sup>80</sup> Zur Verteilung der Daten mittels *P2P-Streaming* wird zumeist das *BitTorrent*-Protokoll verwendet.<sup>81</sup> Zum Austausch der Inhalte bilden die einzelnen Nutzer (*Peers*) ein eigenes Netzwerk. Sämtliche Peers, die sich in einem Netzwerk befinden werden als *Torrent* bezeichnet.<sup>82</sup>

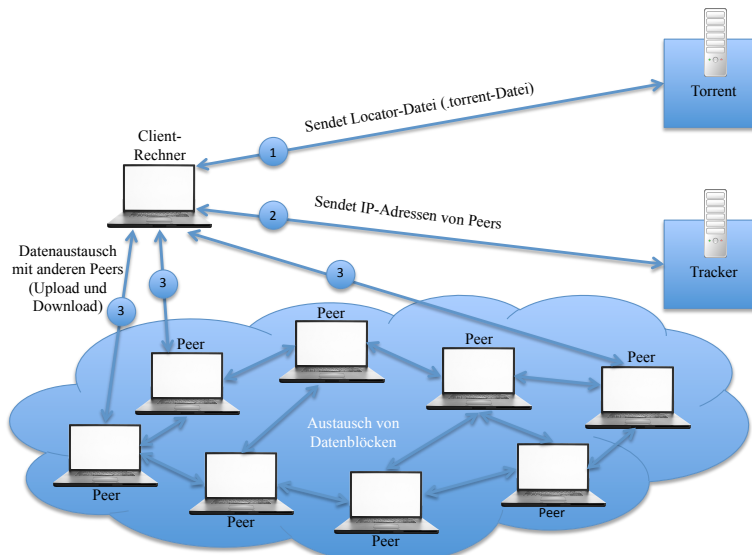


Abbildung 5: Datenverteilung mit BitTorrent, Quellen: KUROSE/ROSS, 172; TANENBAUM/WETHERALL, 850.

<sup>79</sup> WANDTKE/VON GERLACH, GRUR 2013, 682 f.; VON GERLACH, 83, falls das verbindungslose *UDP* verwendet wird, werden die Segmente zudem nicht immer vollständig übertragen.

<sup>80</sup> EISELE, 220 f.; SCHÄUFELE, 38 ff., mit allg. Hinweisen zu *P2P-Netzwerken*; VON GERLACH, 67; BAUMGARTNER, 10 f.

<sup>81</sup> VON GERLACH, 69; <<http://www.bittorrent.com/lang/de>> (besucht 25. August 2015); daneben existieren auch noch andere Protokolle wie etwa die proprietären *Kankan*-Protokolle, vgl. dazu KUROSE/ROSS, 647; SCHÄUFELE, 40 f.

<sup>82</sup> VON GERLACH, 69; TANENBAUM/WETHERALL, 849; SCHWARZENEGGER, ZSR 2008 II, 442 f.

**a) Tracker-Verfahren**

- 30 Das sog. *Tracker*-Verfahren zeichnet sich dadurch aus, dass die IP-Adressen der am P2P-Netzwerk beteiligten Nutzer sowie die Informationen über die jeweils angebotenen Inhalte innerhalb des *Torrents* zentral – von einem sog. *Tracker* als *Server* – verwaltet werden. (1) Um sich mit dem Tracker verbinden zu können, muss sich der Nutzer zunächst eine sog. *Locator*-Datei im Internet besorgen, die zum richtigen *Tracker* führt.<sup>83</sup> Der *Tracker* ist ein *Server*, der die Kommunikation zwischen den verschiedenen Computern (*Peers*) unterstützt, indem er eine Liste all derjenigen *Peers* verwaltet, welche aktiv Inhalte hoch- bzw. herunterladen.<sup>84</sup> Der *Tracker* und die *Locator*-Datei selbst enthalten keine eigenen Inhalte, sondern dienen einzig zum Auffinden und zur Identifikation der Werkdatei.<sup>85</sup> (2) Um Inhalte herunterzuladen, erhält die Client-Software vom *Tracker* eine Liste von *Peers* (*Swarm*) welche die gewünschten Daten bzw. Teile davon haben. (3) In der Folge versucht das Programm mit diesen *Peers* gleichzeitige *TCP*-Verbindungen herzustellen um die Daten herunterzuladen. Zu Beginn besitzt der neue *Peer* noch keine Datenblöcke und lädt zunächst nur Blöcke herunter (*Leecher*). Sobald er Blöcke gesammelt hat, lädt er diese gewöhnlich an andere *Peers* innerhalb des Netzwerks hoch (*Seeder*).<sup>86</sup>

**b) Dezentrales Verfahren**

- 31 Beim dezentralen Verfahren werden anstelle eines *Trackers* sog. *Distributed Hash Tables* (DHTs) verwendet, die eine dezentrale Verteilung der Informationen über einzelne *Clients* ermöglichen.<sup>87</sup> Gegenüber dem *Tracker*-Verfahren hat das dezentrale Verfahren den entscheidenden Vorteil, dass das P2P-Netzwerk nicht von einem zentralen *Tracker* abhängig ist.<sup>88</sup> Im Übrigen unterscheidet sich das dezentrale Verfahren nicht vom *Tracker*-Verfahren.<sup>89</sup>

---

<sup>83</sup> VON GERLACH, 70 ff.

<sup>84</sup> TANENBAUM/WETHERALL, 849.

<sup>85</sup> VON GERLACH, 71.

<sup>86</sup> Vgl. zum Ganzen KUROSE/ROSS, 172 f.; VON GERLACH, 69 ff.; TANENBAUM/WETHERALL, 849.

<sup>87</sup> VON GERLACH, 72.

<sup>88</sup> KUROSE/ROSS, 174 ff.; VON GERLACH, 72.

<sup>89</sup> VON GERLACH, 72 f., m.w.H.

## 2. Streaming von Computerspielen

Das Streaming von Computerspielen steckt derzeit noch in seinen Anfängen, beinhaltet jedoch ein beachtliches Potential: Rechenintensive Computerspiele können auf vergleichsweise leistungsschwachen Endgeräten (wie etwa Smart-TV-Geräte, Tablets und Smartphones) konsumiert werden, da die aufwendigen Berechnungen der Grafik von externen Hochleistungsrechnern übernommen wird.<sup>90</sup> Die Nutzer müssen nicht mehr viel Geld in leistungsstarke Computer oder Spielkonsolen investieren, da bereits eine leistungsstarke Internetverbindung sowie ein internetfähiges Ausgabegerät und allenfalls noch ein zusätzliches Eingabegerät (*Controller*) genügen, um Computerspiele konsumieren zu können. Auch für die Hersteller von Spielkonsolen<sup>91</sup> sprechen gute Gründe für einen Ausbau der Streaming-Dienste: Die Entwicklung und das Marketing für eine neue Spielkonsole verursachen bei den Herstellern hohe Kosten. Teilweise werden die Spielkonsolen sogar unter den Produktionskosten oder nur mit sehr kleinen Gewinnmargen auf den Markt gebracht, um möglichst viele Abnehmer zu finden und so Marktanteile zu gewinnen.<sup>92</sup> Die Refinanzierung erfolgt regelmässig erst durch den Verkauf von Lizenzen an die Spielehersteller<sup>93</sup> sowie bei der Veräusserung eigener Spieletitel und exklusiver Mitgliedschaften. Durch die Zunahme mobiler Geräte kommt der traditionelle Spielkonsolenmarkt zunehmend unter Druck. Das Streaming von Computerspielen stellt deshalb eine Reaktion der Branche auf ein sich veränderndes Marktumfeld dar.

Im Unterschied zum Streaming von Audio-/Video-Dateien, wo der Konsument nur beschränkt auf das Geschehen einwirken kann (Pausieren, Abspielen, Vorwärts- und Zurückspulen), steht beim Spiele-Streaming das interaktive Element im Vordergrund. Der Spieler steuert aktiv das Spielgeschehen. Wird ein Gameplay-Video aufgezeichnet, vermag dieses das Spielerlebnis

<sup>90</sup> Vgl. etwa <<https://www.playstation.com/en-us/explore/playstationnow>> (besucht 25. August 2015), oder <<http://www.nvidia.de/object/nvidia-grid-cloud-gaming-de.html>> (besucht 25. August 2015), die hierfür den Begriff Gaming-as-a-Service (GaaS) verwenden.

<sup>91</sup> Wie etwa Sony, Microsoft und Nintendo.

<sup>92</sup> COUSINS, <<http://kotaku.com/5973498/weapons-of-mass-disruption-3-how-and-why-console-will-die>> (besucht 25. August 2015).

<sup>93</sup> Z.B. Ubisoft Entertainment S.A., Take 2 Interactive, Electronic Arts, Activision Blizzard.

nicht zu ersetzen.<sup>94</sup> Die Gefahr der Herstellung von Raubkopien wird beim Streaming von Computerspielen weitgehend ausgeschaltet, da die Nutzer das Spiel konsumieren können, ohne dass der Anbieter diesen eine vollständige Werkkopie mittels eines physischen Datenträgers (DVD, Blu-ray-Disc etc.) oder Downloads überlassen muss.

### 3. Streaming von Büchern

- 34 Auch im Bereich der *E-Books*<sup>95</sup> haben sich neue Geschäftsmodelle etabliert: Der Bücher-Streaming-Dienst *Readfy*<sup>96</sup> setzt einzig eine funktionierende Internetverbindung voraus, ist für die Nutzer kostenlos und wird durch Werbeeinnahmen finanziert.<sup>97</sup> Bei *Readfy* bleiben die Bücher in der Cloud des Anbieters und können nur innerhalb der App gelesen werden.<sup>98</sup> Es wird kein vollständiges Werkexemplar auf dem Wiedergabegerät des Nutzers abgespeichert.

---

<sup>94</sup> Der Kauf des Live-Streaming-Portals Twitch durch Amazon belegt aber, dass Online-Plattformen, die es den Nutzern ermöglichen, andere Spieler (Profis) zu beobachten und in Foren darüber zu diskutieren, eine nicht zu unterschätzende wirtschaftliche Bedeutung erlangt haben.

<sup>95</sup> Der Begriff *E-Book* steht für ein elektronisches Buch (engl. electronic book) und bezeichnet Bücher in digitaler Form, die auf sog. *E-Book-Readern* (z.B. dem Amazon Kindle), sowie bei Verwendung spezieller Software auch auf Computern, Tablets oder Smartphones gelesen werden können.

<sup>96</sup> <<https://www.readfy.com>> (besucht 25. August 2015).

<sup>97</sup> Die Werbung wird z.B. am Seitenrand eingeblendet, teilweise werden auch ganze Werbespots eingeblendet; vgl. dazu SCHULDT, <<http://www.computerbild.de/artikel/cb-New-s-App-Check-Readfy-eBooks-lesen-zum-Nulltarif-9906451.html>> (besucht 25. August 2015).

<sup>98</sup> STEINHAUS, Streaming-Romane, <<http://digital-heartland.de/readfys-streaming-romane>> (besucht 25. August 2015).

## II. Urheberrechtsschutz

### 1. Rechtsquellen

#### A. Internationales Recht

Auf internationaler Ebene existieren verschiedene Abkommen zum Schutze des Urheberrechts. Als wichtigste Quelle des internationalen Urheberrechts kann die Revidierte Berner Übereinkunft (RBÜ) von 1971 genannt werden, welche in Art. 5 RBÜ den Grundsatz der Inländergleichbehandlung regelt (Assimilationsprinzip) sowie für verbandseigene Werke einen Mindestschutz garantiert.<sup>99</sup> Das TRIPS-Übereinkommen von 1994 regelt handelsbezogene Rechte an geistigem Eigentum.<sup>100</sup> Dieses Übereinkommen gilt zwingend für alle Mitgliedstaaten der WTO und enthält punktuelle Erweiterungen gegenüber dem Schutzniveau der RBÜ.<sup>101</sup> Weiter wurden 1996 die beiden WIPO-Internetabkommen ratifiziert: Der WIPO Copyright Treaty (WCT) und der WIPO Performances and Phonograms Treaty (WPPT).<sup>102</sup> Im Zuge der letzten Revision des Bundesgesetzes über das Urheberrecht und verwandte Schutzrechte (URG) wurden die Schutzlücken des URG gegenüber den beiden WIPO-Internet-Abkommen beseitigt.<sup>103</sup>

#### B. Nationales Recht

Das Schweizer Urheberrechtsgesetz ermöglicht den Rechteinhabern die Ausübung ihrer ideellen und materiellen Interessen am Werk, indem es diesen gewisse Ausschliesslichkeitsrechte einräumt.<sup>104</sup> Der Schutz des Schweizer Urheberrechts unterliegt der Eigentumsgarantie von Art. 26 Abs. 1 BV.<sup>105</sup> Ergänzt wird das URG durch die Ausführungsbestimmungen in der URV.

<sup>99</sup> HILTY, Urheberrecht, Rz. 63 ff.; BORNHAUSER, Rz. 125.

<sup>100</sup> JOLLER, 41; RUBLI, Rz. 35 m.w.H.

<sup>101</sup> HILTY, Urheberrecht, Rz. 67 ff.; RUBLI, Rz. 35.

<sup>102</sup> BECHTOLD, ZSR 2015 II, 78; VON BÜREN/MEER, SIWR II/1, 7 f.; JOLLER, 42; RUBLI, Rz. 133.

<sup>103</sup> HUG, medialex 2014, Fn. 3; CHERPILLOD, SHK URG, Art. 1 N 5; STAUFFACHER, AJP 2008, 1255.

<sup>104</sup> BÖTTCHER, 5; PFORTMÜLLER, SHK URG, Art. 10 N 1; BARRELET/EGLOFF, Art. 10 N 6; REHBINDER/VIGANÒ, Art. 10 N 1.

<sup>105</sup> HILTY, Urheberrecht, Rz. 56.

## 2. Räumlicher Geltungsbereich des schweizerischen Urheberstrafrechts

- <sup>37</sup> Nach Massgabe von Art. 333 Abs. 1 StGB gelten die Allgemeinen Bestimmungen des StGB auch für das Nebenstrafrecht.<sup>106</sup> Folglich bestimmt sich der räumliche Geltungsbereich des schweizerischen Urheberstrafrechts nach den Art. 3 ff. StGB. Gemäss dem in Art. 3 Abs. 1 StGB verankerten Territorialitätsprinzip findet das Schweizer Strafrecht auf alle Delikte Anwendung, die auf schweizerischem Hoheitsgebiet begangen worden sind.<sup>107</sup> Als Begehungsort gilt gemäss Art. 8 Abs. 1 StGB entweder der Ort der Ausführung oder der Ort des Erfolgsintritts der strafbaren Handlung.<sup>108</sup> Sämtliche für das Streaming einschlägigen Urheberrechtsverletzungstatbestände sind als schlichte Tätigkeitsdelikte (Art. 67 und Art. 69 URG) bzw. konkrete oder abstrakte Gefährdungsdelikte (Art. 69a URG) zu qualifizieren.<sup>109</sup> Folglich verbleibt nach h.L. als einziger Anknüpfungspunkt für die Bestimmung der internationalen Zuständigkeit der Ort der Tatausführung.<sup>110</sup> In der Lehre wird teilweise auch die Ansicht vertreten, dass bei den abstrakten Gefährdungsdelikten der Erfolg „in der Schaffung einer Gefahr liege, die sich irgendwie in der Aussenwelt manifestiere“<sup>111</sup>. Bei abstrakten Gefährdungsdelikten, die

---

<sup>106</sup> WIPRÄCHTIGER, BSK StGB II, Art. 333 N 10; TRECHSEL/LIEBER, PK StGB, Art. 333 N 4; DAVID, SHK URG, Vorb. zu Art. 67-73 N 5.

<sup>107</sup> SCHWEINGRUBER, Jusletter vom 10. November 2014, Rz. 1 ff., weist auf die Schwierigkeiten der Cybercrime-Strafverfolgung hin, die das Territorialitätsprinzip bei den grenzüberschreitenden Delikten im Cyberspace verursacht; CHERPILLOD, SIWR II/1, 46, wonach sich der Schutz des URG auch auf Handlungen erstreckt, die „zwar von Personen im Ausland begangen werden, aber in der Schweiz Wirkungen zeitigen; WEBER, E-Commerce, 536; SCHWARZENEGGER, P2P-Netzwerke, 250; ders., E-Commerce, 338.

<sup>108</sup> Zum Handlungs- und Erfolgsort im virtuellen Raum vgl. auch DYENS, 159 ff.; MUGGLI, 187 ff.; SCHWARZENEGGER, E-Commerce, 338.

<sup>109</sup> DAVID, SHK URG, Art. 69a N 9; REHBINDER/VIGANÒ, Art. 69a N 8; SCHWARZENEGGER, ZSR 2008 II, 464; ders., P2P-Netzwerke, 250; ders., E-Commerce, 341 ff.

<sup>110</sup> BALTISSER, 143; WEBER, E-Commerce, 537; FEHLBAUM/LATTMANN, sic! 2009, 377 f.; REHBINDER/VIGANÒ, Art. 69a N 6 ff.; GLARNER, sic! 2006, 648; ders., Musikpiraterie im Internet, 148 ff.

<sup>111</sup> WEBER, E-Commerce, 538; GLARNER, Musikpiraterie im Internet, 150 f., mit einem Vorschlag für eine Neudefinition des Erfolgsdelikts, wonach als Erfolgsort nicht nur jener Ort gilt, „wo ein Erfolg im technischen Sinne eingetreten ist, sondern auch derjenige Ort, an dem die geschützten Interessen verletzt oder gefährdet wurden“; SCHWARZENEGGER, sic! 2001, 247; ders., ZStrR 2000, 124; vgl. ferner auch MUGGLI, 190 f. mit Hinweisen auf Lösungsansätze zur Eingrenzung der Zuständigkeiten bei abstrakten, über das Internet begangenen Gefährdungsdelikten.

über das Internet begangen werden, „sei ein Erfolgsort folglich überall dort anzusiedeln, wo die Gefahr einer Wahrnehmung besteht“<sup>112</sup>. Demnach könnte etwa ein im Ausland handelnder Täter auch in der Schweiz strafrechtlich verfolgt werden, wenn er bspw. vorsätzlich und unrechtmässig Umgehungswerkzeuge nach Art. 69a Abs. 1 lit. b URG über das Internet in Verkehr bringt und diese in der Schweiz abgerufen bzw. heruntergeladen werden können.

### 3. Inhalt des Schweizer Urheberrechts

#### A. Schutzvoraussetzungen

In Art. 2 URG findet sich eine Legaldefinition des Werkbegriffs. Damit der urheberrechtliche Schutz gewährt wird, muss eine „geistige Schöpfung“ der „Literatur oder Kunst“ vorliegen, die sich durch einen „individuellen Charakter“ auszeichnet.<sup>113</sup> Darüber hinausgehende Schutzvoraussetzungen existieren nicht. Insbesondere eine materielle Festlegung des Werks ist nicht erforderlich.<sup>114</sup> Es ist bereits ausreichend, wenn das Werk durch die Sinne objektiv wahrnehmbar ist.<sup>115</sup> Der urheberrechtliche Werkbegriff ist inhaltlich weitgehend deckungsgleich mit demjenigen von Art. 2 Abs. 1 RBÜ.<sup>116</sup> Gemäss Art. 5 Abs. 2 RBÜ sind die Mitgliedstaaten verpflichtet, den urheberrechtlichen Schutz ungeachtet aller Formalitäten zu gewähren. Somit ist weder eine Registrierung, noch ein ausdrücklicher Hinweis erforderlich, um den urheberrechtlichen Schutz zu beanspruchen.<sup>117</sup> Damit eine geistige Schöpfung vorliegt, muss das Werk Ausdruck gedanklicher Tätigkeit eines Menschen sein.<sup>118</sup> Dabei werden keine hohen Anforderungen an die geistige Schöpfungshöhe gestellt.<sup>119</sup> Zwar wird gefordert, dass die geistige Schöpfung im Gegensatz zu

<sup>112</sup> GLARNER, Musikpiraterie im Internet, 151; ausführlich dazu SCHWARZENEGGER, sic! 2001, 248 ff.; ders., E-Commerce, 344 f.; ders., ZStrR 2000, 125.

<sup>113</sup> CHERPILLOD, SHK URG, Art. 2 N 1; HILTY, Urheberrecht, Rz. 83; THOUVENIN, FS-Hilty, 62 ff.; BARRELET/EGLOFF, Art. 2 N 4; GLARNER, Musikpiraterie im Internet, 57 ff.

<sup>114</sup> CHERPILLOD, SHK URG, Art. 2 N 3; BARRELET/EGLOFF, Art. 2 N 4.

<sup>115</sup> CHERPILLOD, SHK URG, Art. 2 N 3; BARRELET/EGLOFF, Art. 2 N 4; DESSMONTET, droit d'auteur, 31 f.

<sup>116</sup> BARRELET/EGLOFF, Art. 2 N 3.

<sup>117</sup> CHERPILLOD, SHK URG, Art. 2 N 8; BARRELET/EGLOFF, Art. 1 N 2.

<sup>118</sup> CHERPILLOD, SHK URG, Art. 2 N 9; HILTY, Urheberrecht, Rz. 83; BARRELET/EGLOFF, Art. 2 N 5; BGE 130 III 168, Erw. 4.5.

<sup>119</sup> CHERPILLOD, SHK URG, Art. 2 N 9; BARRELET/EGLOFF, Art. 2 N. 5 f.;

einer Kopie „etwas Neues“ darstellen muss – der Grad der Neuheit kann jedoch auch sehr gering ausfallen.<sup>120</sup> Weiter muss die geistige Schöpfung den Bereichen der Literatur oder der Kunst angehören, wobei diese Begriffe in einem extrem weiten Sinne verstanden werden.<sup>121</sup> Schliesslich muss das Werk einen individuellen Charakter aufweisen: Dabei steht die geforderte Individualität in Relation zum Gestaltungsspielraum des Urhebers.<sup>122</sup> Die Frage, ob ein Werk die erforderliche Individualität erreicht, stets bloss relativ bestimmt werden, indem das konkrete Werk mit anderen Schöpfungen derselben Werksgattung verglichen wird.<sup>123</sup>

## **B. Rechte des Urhebers**

- 39 Das Schweizer Urheberrecht folgt dem Schöpferprinzip, was bedeutet, dass der Urheber sämtliche Rechte an seinem Werk erwirbt, ohne dass hierfür ein gesonderter formaler Akt notwendig ist.<sup>124</sup> Urheber i.S.v. Art. 6 URG ist diejenige natürliche Person, die das Werk geschaffen hat.<sup>125</sup> Die Rechte des Urhebers bestehen aus zwei Komponenten: den Vermögensrechten (auch Nutzungs- und Verwertungsrechte genannt) und den Urheberpersönlichkeitsrechten.<sup>126</sup> Die Urheberpersönlichkeitsrechte sind grundsätzlich nicht übertragbar und umfassen das Recht auf Anerkennung der Urheberschaft (Art. 9 Abs. 1 URG), das Recht auf Erstveröffentlichung (Art. 9 Abs. 2 URG) sowie das Recht auf Werkintegrität (Art. 11 URG).<sup>127</sup> Gestützt auf die in Art. 10

---

<sup>120</sup> CHERPILLOD, SHK URG, Art. 2 N 9, mit dem Hinweis, dass sämtliche Werke gewisse vorbestehende Elemente verwenden; BARRELET/EGLOFF, Art. 2 N 6; HILTY, Urheberrecht, Rz. 85, plädiert dafür, dass etwas noch nicht Vorhandenes geschaffen werden muss; kritisch BECHTOLD, ZSR 2015 II, 94, weist darauf hin, dass sich geringe Schutzanforderungen allenfalls negativ auf die kreative Produktivität auswirken können.

<sup>121</sup> CHERPILLOD, SHK URG, Art. 2 N 11; BARRELET/EGLOFF, Art. 2 N 6, mit Verweis auf die weit gefasste Aufzählung in Art. 2 Abs. 2 URG.

<sup>122</sup> CHERPILLOD, SHK URG, Art. 2 N 15 ff.; BARRELET/EGLOFF, Art. 2 N 8a, m.w.H.; GLARNER, Musikpiraterie im Internet, 58 f.; a.A. HILTY, Urheberrecht, Rz. 92 f., der hierdurch den Sinn der Schutzvoraussetzung der Individualität unterlaufen sieht. Der Autor plädiert dafür, die Anforderungen an die Individualität nicht zu tief anzusetzen, um eine Überdehnung des Schutzbereichs des Urheberrechts zu verhindern.

<sup>123</sup> Siehe dazu THOUVENIN, FS-Hilty, 73.

<sup>124</sup> HUG, SHK URG, Art. 6 N 1; HILTY, Urheberrecht, Rz. 131 f.; Botschaft URG 1989, 525.

<sup>125</sup> HUG, SHK URG, Art. 6 N 3; BARRELET/EGLOFF, Art. 6 N 1 f.; REHBINDER, 119.

<sup>126</sup> HILTY, Urheberrecht, Rz. 149.

<sup>127</sup> BECHTOLD, ZSR 2015 II, 81 f., m.w.H.; DESSEMONTET, SIWR II/1, 182 ff.; RIGAMONTI, Urheberpersönlichkeitsrechte, 13 ff.; BOSSHART, 90 ff.; PFORTMÜLLER, SHK URG, Art. 11 N 1; CSOPORT, 57; BARRELET/EGLOFF, Art. 9 N 7; REHBINDER/VIGANÒ, Art. 11 N 1.



Abs. 1 URG verankerten Vermögensrechte wird dem Urheber das ausschliessliche Recht erteilt, darüber zu bestimmen, ob, wann und wie das Werk verwendet wird. Dadurch soll dem Urheber eine angemessene Vergütung gesichert werden.<sup>128</sup> Der Urheber kann die Rechte an seinem Werk auch abtreten sowie eine exklusive oder nicht exklusive Lizenz erteilen.<sup>129</sup>

### C. Verwandte Schutzrechte (Art. 33 ff. URG)

Die in Art. 33 ff. URG geregelten verwandten Schutzrechte, auch Leistungs- 40  
schutzrechte oder Nachbarrechte genannt, schützen die ausübenden Künstler (Interpreten), die Hersteller von Ton- und Bildträgern (Produzenten) sowie die Sendeunternehmen (Werkvermittler), indem diesen selbständige Verbotsrechte bzw. Vergütungsansprüche gegenüber Dritten gewährt werden.<sup>130</sup> Falls eine Kopie eines urheberrechtlich geschützten Werks hergestellt wird, können etwa das Vervielfältigungsrecht der ausübenden Künstler (Art. 33 Abs. 2 lit. c URG), das Vervielfältigungsrecht der Hersteller von Ton- und Tonbildträgern (Art. 36 lit. a URG) und das Vervielfältigungsrecht zum Schutze der Sendeunternehmen (Art. 37 lit. c URG) berührt sein. Wird ein digitales Werk auf Abruf (On-Demand) zum Streaming angeboten, können zudem das Recht auf öffentliche Zugänglichmachung zum Schutz der Künstler nach Art. 33 Abs. 2 lit. a URG, jenes zum Schutz der Hersteller von Ton- und Tonbildträgern gem. Art. 36 lit. b URG sowie jenes zum Schutz der Sendeunternehmen nach Art. 37 lit. e URG tangiert sein. Die vorsätzliche und unrechtmässige Verletzung von verwandten Schutzrechten wird gemäss Art. 69a Abs. 1 URG auf Antrag der verletzten Person mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft. Bei gewerbsmässiger Begehung wird die Tat von Amtes wegen verfolgt und mit einer Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft. Art. 69 URG ist analog zu Art. 67 URG aufgebaut. Um eine bessere Übersicht über die Materie behalten zu können, wird im weiteren Verlauf dieser Arbeit auf eine gesonderte Darstellung der verwandten Schutzrechte in der rechtlichen Bewertung der einzelnen Vorgänge beim Streaming weitestgehend verzichtet. Die Art. 69 und Art. 67

<sup>128</sup> HILTY, Urheberrecht, Rz. 149; BARRELET/EGLOFF, Art. 10 N 1 ff.

<sup>129</sup> PFORTMÜLLER, SHK URG, Art. 10 N 1 ff.

<sup>130</sup> MOSIMANN, SIWR II/1, 334 ff., m.w.H.; AUF DER MAUR, SHK URG, N 1 Vorb. zu Art. 33-39; BARRELET/EGLOFF, Art. 33 N 1; REHBINDER/VIGANÒ, Art. 10 N 19; GLARNER, Musikpiraterie im Internet, 44 ff.; WILD, Jusletter vom 17. Dezember 2001, Rz. 10 f.; HILTY, UFITA 1994, 91 ff.

URG weisen unterschiedliche Schutzbereiche auf, weshalb sie in echter Konkurrenz zueinander stehen.<sup>131</sup>

## D. Schranken des Urheberrechts

- 41 Im fünften Kapitel<sup>132</sup> des schweizerischen Urheberrechtsgesetzes werden unter dem Titel „Schranken des Urheberrechts“ zahlreiche Einschränkungen der urheberrechtlichen Schutzrechte aufgeführt.<sup>133</sup> Mit dem vom Gesetzgeber eingeführten System der Schrankenregelung im Urheberrecht wird das Ziel verfolgt, noch während der Dauer der Schutzfrist<sup>134</sup>, einen differenzierten Ausgleich zwischen den widerstreitenden Interessen der Rechteinhaber (Verwerter), der Urheber, der Werknutzer und der Allgemeinheit zu erzielen.<sup>135</sup> HILTY spricht daher auch von einem Instrument zur „Feinjustierung“ innerhalb des Verbotsbereichs.<sup>136</sup> Einerseits sollen gewisse Handlungen mit urheberrechtlich geschützten Werken nicht einfach verboten werden (z.B. die Parodie; Art. 11 Abs. 3 URG) und andererseits ist an die unkontrollierbare Massennutzung zu denken. Eine Überprüfung sämtlicher Privathaushalte auf unrechtmässige Privatkopien wäre nicht nur ein absolut unverhältnismässiger Eingriff in die Privatsphäre der Bürger, sondern darüber hinaus in der Praxis weder umsetzbar noch aus ökonomischer Sicht sinnvoll.<sup>137</sup> Damit die Rechteinhaber für die Nutzung ihrer Werke dennoch eine Entschädigung

---

<sup>131</sup> DAVID, SHK URG, Art. 69 N 3a; BARRELET/EGLOFF, Art. 69 N 1; SCHWARZENEGGER, P2P-Netzwerke, 215 f.; GLARNER, Musikpiraterie im Internet, 90 ff.

<sup>132</sup> Art. 19-28 URG.

<sup>133</sup> BOSSHART, 107, m.w.H.; GASSER/OERTLI, SHK URG, N 1 ff. Vorb. zum 5. Kapitel, mit dem Hinweis, dass auch in anderen Kapiteln des Gesetzes noch vereinzelt Schrankenregelungen verankert sind, z.B. das Parodierecht (Art. 11 Abs. 3 URG) oder das Vermietrecht (Art. 13 Abs. 1-3 URG); GIRSBERGER, 190; BECHTOLD, Informationsgesellschaft, 71; BÜHLER, 253.

<sup>134</sup> Vgl. zur Regelung der Schutzdauer die Art. 29-32 URG; siehe auch BAUMGARTNER, 52, der darauf hinweist, dass dem Schöpfer nur zeitlich befristete Exklusivrechte an der Werkverwertung gewährt werden und nach Ablauf der Schutzdauer das Werk den Status eines frei nutzbaren Allgemeinguts erlangt.

<sup>135</sup> GASSER/OERTLI, SHK URG, N 4 ff. Vorb. zum 5. Kapitel; BARRELET/EGLOFF, Art. 19 N 2 ff.; REHBINDER/VIGANÒ, Art. 19 N 5; GEIGER, FS-Hilty, 82, „der Inhalt des Ausschliesslichkeitsrechts wird durch seine Schranken bestimmt. Über diese Grenzen hinaus hat der Urheber keine Kontrollmöglichkeit mehr“.

<sup>136</sup> HILTY, Urheberrecht, Rz. 210 f.

<sup>137</sup> BIELER, sic! 2015, 163 f.; BARRELET/EGLOFF, Art. 19 N 5 ff.; REHBINDER/VIGANÒ, Art. 19 N 12.

erhalten, wurden die sog. Verwertungsgesellschaften geschaffen, welche bestimmte Gebühren erheben (wie z.B. die Leerträgervergütung auf beispielbare DVDs oder CDs) und diese anschliessend mittels eines Umlageverfahrens an die Rechteinhaber ausschütten.<sup>138</sup> BAUMGARTNER weist darauf hin, dass der Schöpfer eines Werks – anders als der Eigentümer einer Sache – die Nutzung durch Dritte beabsichtigt, um dadurch Einkünfte zu generieren bzw. seinen Bekanntheitsgrad zu steigern.<sup>139</sup> Im digitalen Umfeld wird der Unterschied zwischen urheberrechtlich geschützten, digitalen Werken und dem Sacheigentum besonders deutlich, da die digitalen Werke kopiert und parallel genutzt werden können, ohne dass dadurch die Nutzung des Originals beeinträchtigt wird.<sup>140</sup> Die nachfolgende Abbildung soll eine Übersicht über die verschiedenen Arten von Schranken vermitteln<sup>141</sup>:

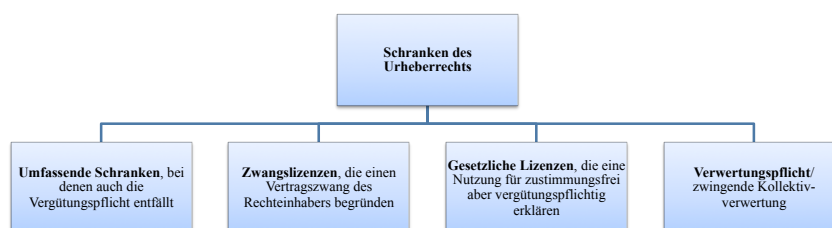


Abbildung 6: Übersicht über die verschiedenen Schranken des Urheberrechts

- *Umfassende Schranken:*  
Bei den umfassenden Schranken werden gewisse Werkverwendungen vom Urheberrechtsschutz ausgenommen und dürfen zustimmungsfrei und ohne Bezahlung einer Vergütung genutzt werden (Art. 11 Abs. 3; Art. 13 Abs. 3; Art. 19 Abs. 1 lit. a unter Vorbehalt von Art. 19 Abs. 2 und Art. 20 Abs. 2 und 3; Art. 21; Art. 22 Abs. 2; Art. 24; Art. 24a; Art. 24c Abs. 3 letzter Satzteil; Art. 25-28 URG).<sup>142</sup>

<sup>138</sup> Vgl. zum Ganzen HILTY, Urheberrecht, Rz. 210 f.

<sup>139</sup> BAUMGARTNER, 53.

<sup>140</sup> THOUVENIN, NZZ, 19; BAUMGARTNER, 53.

<sup>141</sup> GASSER/OERTLI, SHK URG, N 2 Vorb. zum 5. Kapitel; HILTY, Urheberrecht, Rz. 211; BARRELET/EGLOFF, Art. 19 N 2; GASSER, 8.

<sup>142</sup> GASSER/OERTLI, SHK URG, N 2 Vorb. zum 5. Kapitel; BARRELET/EGLOFF, Art. 19 N 2; REHBINDER/VIGANÒ, Art. 19 N 6; GASSER, 8.

- *Zwangslizenzen:*  
Bei der Zwangslizenz ist der Rechtsinhaber vertraglich verpflichtet, mit den Nutzern einen individuellen Lizenzvertrag abzuschliessen, wobei dieser an angemessene Bedingungen geknüpft werden darf (Art. 23 URG).<sup>143</sup>
- *Gesetzliche Lizenzen:*  
Die gesetzlichen Lizenzen erlauben eine zustimmungsfreie Nutzung urheberrechtlich geschützter Werke, verbinden diese aber mit einer Vergütungspflicht (Art. 13 Abs. 1 und 3; Art. 19 Abs. 1 lit. a i.V.m. Art. 19 Abs. 2 lit. b und c und Art. 19 Abs. 2 i.V.m. Art. 20 Abs. 2 und 3; Art. 24c unter Vorbehalt von Art. 24c Abs. 3 letzter Satzteil; Art. 35 URG).<sup>144</sup>
- *Verwertungsgesellschaftspflicht / zwingende Kollektivverwertung:*  
Die Verwertungsgesellschaftspflicht lässt den Inhalt der Schutzrechte unberührt, beschränkt aber deren individuelle Ausübung durch eine kollektive Wahrnehmung über die Verwertungsgesellschaften (Art. 22 Abs. 1; Art. 22a Abs. 1 unter Vorbehalt von Art. 22a Abs. 3; Art. 22b; Art. 22c; Art. 24b URG).<sup>145</sup>

## **E. Rechtsschutz**

### **a) Zivilrechtlicher Schutz**

- 42 Bei Verstössen gegen das Urheberrecht können die Rechteinhaber zivilrechtliche Ansprüche nach Art. 61 f. URG gegen die Urheberrechtsverletzer geltend machen.<sup>146</sup> Neben der Feststellungsklage<sup>147</sup> (Art. 61 URG) stehen den Betroffenen als Abwehrklagen der Unterlassungs- und Beseitigungsanspruch

---

<sup>143</sup> GASSER/OERTLI, SHK URG, N 2 Vorb. zum 5. Kapitel; GASSER, SHK URG, Art. 24 N 2 ff.; BARRELET/EGLOFF, Art. 23 N 1; REHBINDER/VIGANÒ, Art. 23 N 1.

<sup>144</sup> GASSER/OERTLI, SHK URG, N 2 Vorb. zum 5. Kapitel; BARRELET/EGLOFF, Art. 19 N 2; REHBINDER/VIGANÒ, Art. 19 N 4; GASSER, 8.

<sup>145</sup> GASSER/OERTLI, SHK URG, N 2 Vorb. zum 5. Kapitel; BARRELET/EGLOFF, Art. 19 N 2; REHBINDER/VIGANÒ, Art. 19 N 4.

<sup>146</sup> HUG, medialex 2014, 55; MÜLLER, SHK URG, Art. 61 N 3 ff.; ausführlich zum zivilrechtlichen Schutz CSOPORT, 57 ff.

<sup>147</sup> Siehe MÜLLER, SHK URG, Art. 61 N 3 ff.

(Art. 62 Abs. 1 lit. a und b URG) zur Verfügung.<sup>148</sup> Gestützt auf Art. 62 Abs. 2 URG kann der betroffene Rechteinhaber zudem auf Schadenersatz klagen oder alternativ die Herausgabe des widerrechtlich erzielten Gewinnes sowie eine Genugtuung verlangen.<sup>149</sup>

### **b) Strafrechtlicher Schutz**

Durch die Art. 67 ff. URG wird der zivilrechtliche Schutz gegen Verletzungen durch Strafbestimmungen ergänzt. Diese umfassen nebst Verstössen gegen die Urheberrechte und die verwandten Schutzrechte auch Verletzungen des Schutzes technischer Massnahmen. Urheberrechtsverletzungen sind nur bei vorsätzlicher Tatbegehung strafbar, wobei Eventualvorsatz genügt.<sup>150</sup> Mit Ausnahme von Art. 70 URG sind sämtliche Grundtatbestände (Art. 67 Abs. 1, Art. 68, Art. 69 Abs. 1 und Art. 69a Abs. 1) als Antragsdelikte konzipiert.<sup>151</sup> Eine Strafverfolgung von Amtes wegen ist nur bei gewerbsmässiger Begehung (Art. 67 Abs. 2, Art. 69 Abs. 2 und Art. 69a Abs. 2) sowie bei Art. 70 URG vorgesehen.<sup>152</sup> Da die einzelnen Straftatbestände von Art. 67 und Art. 69 URG unterschiedliche Rechtsgüter schützen, stehen sie in echter Konkurrenz zueinander.<sup>153</sup>

Nach Art. 333 Abs. 1 StGB sind die Allgemeinen Bestimmungen des Strafgesetzbuches auf alle Taten anwendbar, die in andern Bundesgesetzen mit Strafe bedroht sind, soweit diese keine eigenen Bestimmungen enthalten.<sup>154</sup> Mangels abweichender Regelungen hinsichtlich des materiellen Legalitäts-

<sup>148</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 57 ff.; CSOPORT, 59 ff.; BAUMGARTNER, 208 f.

<sup>149</sup> HUG, medialex 2014, 55; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 70 ff., m.w.H.; BARRELET/EGLOFF, Art. 62 N 14, mit dem Hinweis, dass ein Genugtuungsanspruch einzig im Falle einer Verletzung der Urheberpersönlichkeit gestützt auf Art. 49 OR denkbar sei; zur Rechtslage in Deutschland siehe HEWICKER/MARQUARDT/NEURAUTER, NJW 2014, 2753 ff., mit Hinweisen zum Abmahnkostenersatzanspruch nach UrhG.

<sup>150</sup> DAVID, SHK URG, N 5 Vorb. zu Art. 67-73; REHBINDER/VIGANÒ, Art. 67 N 2; GLARNER, Musikpiraterie im Internet, 87 f.

<sup>151</sup> DAVID, SHK URG, N 7 Vorb. zu Art. 67-73; REHBINDER/VIGANÒ, Art. 67 N 3; GLARNER, Musikpiraterie im Internet, 69.

<sup>152</sup> REHBINDER/VIGANÒ, Art. 67 N 3; GLARNER, Musikpiraterie im Internet, 69.

<sup>153</sup> DAVID, SHK URG, Art. 69 N 3a; BARRELET/EGLOFF, Art. 69 N 1; SCHWARZENEGGER, P2P-Netzwerke, 215 f.; GLARNER, Musikpiraterie im Internet, 90 ff.

<sup>154</sup> WIPRÄCHTIGER, BSK StGB II, Art. 333 N 10; TRECHSEL/CRAMERI, PK StGB, Art. 333 N 4; CSOPORT, 64.

prinzips (Art. 1 StGB), des Territorialitätsprinzips bzw. Strafanwendungsrechts (Art. 3 ff. StGB), der Teilnahme (Art. 24-26 StGB), der persönlichen Verhältnisse (Art. 27 StGB), des Strafantrags (Art. 30-33 StGB) sowie der Einziehung (Art. 69) sind die Allgemeinen Bestimmungen des Strafgesetzbuches auf die Tatbestände von Art. 67, 69 und 69a URG anwendbar.<sup>155</sup> Der Gerichtsstand bestimmt sich nach Art. 31 ff. StPO. Gemäss Art. 71 URG sind bei Widerhandlungen in Geschäftsbetrieben, durch Beauftragte und dergleichen die Sonderbestimmungen des Verwaltungsstrafgesetzes anwendbar (Art. 6 und 7 VStrR).<sup>156</sup>

---

<sup>155</sup> DAVID, SHK URG, N 11 f. Vorb. zu Art. 67-73; BARRELET/EGLOFF, Art. 67 N 2; SCHWARZENEGGER, ZSR 2008 II, 462; ders., P2P-Netzwerke, 216; GLARNER, Musikpiraterie im Internet, 66.

<sup>156</sup> DAVID, SHK URG, N 14 zu Vorb. zu Art. 67-73.

## **2. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Stream-Anbieters**

### **I. Betroffene Verwertungsrechte**

In diesem Teil der Arbeit wird das Augenmerk auf die rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten digitalen Werken aus Sicht des Stream-Anbieters gerichtet. Konkret wird untersucht, welche der in Art. 10 URG statuierten ausschliesslichen Verwertungsrechte die Stream-Anbieter für die Verwertung von urheberrechtlich geschützten Werken von den Rechteinhabern einholen müssen. Dabei ist jeweils zu differenzieren, ob die Werke mittels nicht-linearen Streamings (On-Demand-Streaming) oder linearen Streamings (Live-Streaming, Near-on-Demand-Streaming) gesendet werden. 45

#### **1. Vervielfältigungsrecht (Art. 10 Abs. 2 lit. a URG)**

Die Urheber haben das ausschliessliche Recht, ihre Werke auf beliebigen Trägermedien festzuhalten und Kopien ihrer Werkexemplare herzustellen, solange keine Schrankenregelung greift.<sup>157</sup> Dabei ist strittig, ob von der Formulierung von Art. 10 Abs. 2 lit. a URG nur körperliche Werkexemplare erfasst werden.<sup>158</sup> Nach hier vertretener Auffassung sollte der Ausdruck „Werkexemplar“ weit ausgelegt werden, da es nicht entscheidend sein kann, ob das digitale Werkexemplar fest mit einem Datenträger verbunden ist (CD-ROM, DVD, 46

---

<sup>157</sup> BERANEK ZANON/DE LA CRUZ BÖHRINGER, sic! 2013, 672; PFORTMÜLLER, SHK URG, Art. 10 N 5; HILTY, Urheberrecht, Rz. 156; WEBER, E-Commerce, 267 f.; BARRELET/EGLOFF, Art. 10 N 12; DESSEMONTET, droit d’auteur, 169 ff.; zu den Rechten der ausübenden Künstler und der Hersteller von Ton- oder Tonbildträgern vgl. Art. 33 Abs. 2 lit. c URG bzw. Art. 36 lit. a URG.

<sup>158</sup> DAVID, SHK URG, Art. 67 N 13; SCHWARZENEGGER, P2P-Netzwerke, 217, der dafür plädiert, auch die Vervielfältigung unkörperlicher Werkwiedergaben unter diesen Tatbestand zu subsumieren.

Blu-Ray-Disc etc.) oder nicht (Festplatte, Cloud-Speicher etc.).<sup>159</sup> Umfasst werden sämtliche körperlichen wie auch unkörperlichen Vervielfältigungen, selbst wenn diese bloss von vorübergehender Natur sind.<sup>160</sup>

## **A. Nicht-lineares Streaming**

- 47 Beim nicht-linearen Server-Streaming (On-Demand-Streaming) ist vorgängig eine vollständige Speicherung des digitalisierten, codierten, komprimierten und in das geeignete Format konvertierten Streams auf einem *Server* erforderlich.<sup>161</sup> Dieser Vorgang fällt unter das in Art. 10 Abs. 2 lit. a URG statuierte Vervielfältigungsrecht.<sup>162</sup> Damit der Stream-Anbieter ein Werk auf dem Wege des nicht-linearen Streaming verbreiten darf, muss er deshalb vorgängig die Einwilligung der Rechteinhaber zur Herstellung einer Werkvervielfältigung einholen.

## **B. Lineares Streaming**

### **a) Live-Streaming**

- 48 Beim Live-Streaming werden die Audio-/Video-Inhalte in Echtzeit codiert und direkt nach der Aufnahme über den *Media-Server* an die jeweiligen Media-Player weitergeleitet.<sup>163</sup> Eine vorgängige, vollständige Vervielfältigung der Mediendatei auf einem *Server* ist nicht erforderlich.<sup>164</sup>
- 49 Damit eine Audio-/Videodatei mittels Live-Streaming an die Nutzer verbreitet werden kann, sind – technisch bedingt – dennoch kurzzeitige digitale

---

<sup>159</sup> SCHWARZENEGGER, P2P-Netzwerke, 217; BARRELET/EGLOFF, Art. 10 N 12; REHBINDER/VIGANÒ, Art. 10 N 7; a.A. BÜHLER, 149 ff.

<sup>160</sup> PFORTMÜLLER, SHK URG, Art. 10 N 5; BARRELET/EGLOFF, Art. 10 N 12; BÜHLER, 157 ff.; HILTY, Urheberrecht, Rz. 156; SCHWARZENEGGER, P2P-Netzwerke, 225; kritisch DAVID, SHK URG, Art. 67 N 13.

<sup>161</sup> VON APPEN/BARATH, CaS 2014, 250; SCHÄUFELE, 99; VON GERLACH, 53; EICHELBERGER, 28; RADMANN, ZUM 2010, 388; KOCH, GRUR 2010, 574.

<sup>162</sup> Zum deutschen Recht KOCH, GRUR 2010, 576; BÜSCHER/MÜLLER, GRUR 2009, 559.

<sup>163</sup> VON GERLACH, 51; BÜSCHER/MÜLLER, GRUR 2009, 559; LONGOLIUS, 50.

<sup>164</sup> VON APPEN/BARATH, CaS 2014, 253, „gewöhnlich finden auch beim Live-Streaming kurzzeitige Abspeicherungen des Inhalts auf dem *Server* des Anbieters [statt], der Inhalt [wird] so um wenige Sekunden zeitversetzt an die Nutzer weitergereicht“; EICHELBERGER, 28; BÜSCHER/MÜLLER, GRUR 2009, 559.



Vervielfältigungen auf einem *Server* erforderlich.<sup>165</sup> Sofern die gestreamte Mediendatei die Anforderungen an ein Werk i.S.v. Art. 2 URG erfüllt, ist davon auszugehen, dass bereits die Vervielfältigung von einigen wenigen Sekunden dieser Datei ausreicht, um einen Eingriff in das Vervielfältigungsrecht der Rechteinhaber anzunehmen.<sup>166</sup>

Im Einzelfall ist die Bewertung der Schöpfungshöhe der beim Live-Streaming auf den *Servern* hergestellten vorübergehenden Vervielfältigungen mit praktischen Schwierigkeiten behaftet, da sich diese erst rückblickend beurteilen lässt und die Vervielfältigungen normalerweise bereits während der Werkwiedergabe wieder gelöscht bzw. überschrieben werden.<sup>167</sup> M.E. zu Recht plädiert deshalb ein Teil der Lehre dafür, dass nicht auf die Schutzfähigkeit des konkret zwischengespeicherten Werkteils abgestellt werden sollte, sondern dass „auch die sukzessive, chronologisch geordnete, auch nur flüchtige Vervielfältigung von an sich nicht schutzfähigen Werkteilen [als rechtlich relevante Vervielfältigung aufgefasst werden muss], solange in der Gesamtbetrachtung das ganze Werk oder schutzfähige Teile davon vervielfältigt werden“<sup>168</sup>. Daher sollte auch beim Live-Streaming die Einwilligung der Rechteinhaber zur Herstellung einer Werkvervielfältigung i.S.v. Art. 10 Abs. 2 lit. a URG eingeholt werden.

#### **b) *Near-on-Demand-Streaming***

Beim Near-On-Demand-Streaming werden bereits bestehende Audio-/Video-Inhalte in regelmässigen Intervallen an die Nutzer übertragen.<sup>169</sup> Anders als beim Live-Streaming, bei dem eine vorgängige Vervielfältigung der Aufnahme nicht zwingend erforderlich ist, werden hier bereits produzierte Inhalte verbreitet. Deshalb ist auch beim Near-on-Demand-Streaming eine vor-

<sup>165</sup> VON APPEN/BARATH, CaS 2014, 253 f.; EICHELBERGER, 28, 30 f.; a.A. BÜSCHER/MÜLLER, GRUR 2009, 559.

<sup>166</sup> VON APPEN/BARATH, CaS 2014, 254; BARRELET/EGLOFF, Art. 10 N 12; REHBINDER/VIGANÒ, Art. 10 N 8.

<sup>167</sup> Ausführlich zur Schutzfähigkeit von Teilvervielfältigungen vgl. Rz. 163 ff.; MAY, 174; ENSTHALER, NJW 2014, 1554; GALETZKA/STAMER, MMR 2014, 294 f.; WANDTKE/VON GERLACH, GRUR 2013, 678; VON GERLACH, 113 ff.; STOLZ, MMR 2013, 355; STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 499.

<sup>168</sup> STOLZ, MMR 2013, 355; gl.M. ENSTHALER, NJW 2014, 1554; WANDTKE/VON GERLACH, GRUR 2013, 683; VON GERLACH, 212 ff.; OĞLAKCIOĞLU, ZIS 2012, 436; FANGEROW/SCHULZ, GRUR 2010, 678; a.A. MAY, 172; SCHEDER-BIESCHIN, 167; kritisch GALETZKA/STAMER, MMR 2014, 294 f.; STIEPER, MMR 2012, 13 f.

<sup>169</sup> VON GERLACH, 52.

gängige Abspeicherung der Audio-/Video-Inhalte auf einem *Server* erforderlich. Damit ein Stream-Anbieter geschützte Audio-/Video-Inhalte mittels Near-on-Demand-Streaming verbreiten darf, muss er zuvor von den Rechteinhabern die Einwilligung zur Herstellung einer Werkvervielfältigung einholen.

## 2. Recht der Zugänglichmachung (Art. 10 Abs. 2 lit. c URG)

- 52 Art. 10 Abs. 2 lit. c URG verleiht den Urhebern das Recht, ihre Werke für ein Publikum wahrnehmbar zu machen, indem sie es vortragen, aufführen, vorführen oder so zugänglich machen, dass Personen von Orten und Zeiten ihrer Wahl dazu Zugang haben.<sup>170</sup> Anders als beim Senderecht nach Art. 10 Abs. 2 lit. d URG hält der Anbieter bei der öffentlichen Zugänglichmachung das Werk zum Abruf bereit. Dabei ist es irrelevant, ob das Werk auch tatsächlich abgerufen und wahrgenommen wird.<sup>171</sup> Der Nutzer selbst bestimmt durch seinen Abruf individuell über den Zeitpunkt der Wiedergabe.<sup>172</sup> Das öffentliche Zugänglichmachen urheberrechtlich geschützter Werke unterliegt der kumulativen Einwilligung der Rechteinhaber sowohl für den Ort, an dem das Werk zum Abruf bereit gehalten wird (*Serverstandort*), wie auch für sämtliche Gebiete, in denen der Werkzugang möglich ist.<sup>173</sup>

### A. Nicht-lineares Streaming

- 53 Das nicht-lineare Streaming zeichnet sich dadurch aus, dass der Anbieter das Werk für den Nutzer auf Abruf bereit hält und dieser selbst über den Zeit-

---

<sup>170</sup> DESSEMONTET, SIWR II/1, 199 ff.; BERANEK ZANON/DE LA CRUZ BÖHRINGER, sic! 2013, 673 f.; BOSSHART, 107 f.; BRÄNDLI/TAMÒ, sic! 2013, 655; PFORTMÜLLER, SHK URG, Art. 10 N 10; HILTY, Urheberrecht, Rz. 169; VON GERLACH, 53; WEBER, E-Commerce, 270; BARRELET/EGLOFF, Art. 10 N 19 f.

<sup>171</sup> BERANEK ZANON/DE LA CRUZ BÖHRINGER, sic! 2013, 673; REHBINDER/VIGANÒ, Art. 10 N 19.

<sup>172</sup> BARRELET/EGLOFF, Art. 10 N 22a; BRÄNDLI/TAMÒ, sic! 2013, 655 f. m.w.N.; EICHELBERGER, 23.

<sup>173</sup> REHBINDER/VIGANÒ, Art. 10 N 19; durch den Einsatz sog. Geo-Sperren lässt sich die Abrufbarkeit des Angebots territorial auf bestimmte Gebiete einschränken, vgl. dazu Rz. 269 ff.

punkt bestimmen kann, an dem er das Werk konsumieren will.<sup>174</sup> Das Bereithalten urheberrechtlich geschützter Werke zum Abruf durch die Nutzer erfüllt den Tatbestand der öffentlichen Zugänglichmachung gemäss Art. 10 Abs. 2 lit. c URG.<sup>175</sup> Die Verwertung eines urheberrechtlich geschützten Werks auf dem Wege des nicht-linearen Streaming setzt daher voraus, dass der Stream-Anbieter über eine Einwilligung für eine Zugänglichmachung nach Art. 10 Abs. 2 lit. c URG verfügt.

## B. Lineares Streaming

Da sowohl beim Live-Streaming als auch beim Near-on-Demand-Streaming nicht die Nutzer selbst, sondern die Anbieter über den Zeitpunkt der Wiedergabe entscheiden, ist das Recht der öffentlichen Zugänglichmachung nach Art. 10 Abs. 2 lit. c URG nicht tangiert.<sup>176</sup>

## 3. Senderecht (Art. 10 Abs. 2 lit. d URG)

Art. 10 Abs. 2 lit. d URG räumt den Urhebern das Recht ein, ihre Werke über Radio, Fernsehen oder ähnliche Einrichtungen zu senden. Das Senderecht regelt die Massenkommunikation, bei welcher derselbe Sendeinhalt zeitgleich an eine mehr oder weniger grosse Zahl von Personen übermittelt wird.<sup>177</sup> In Abgrenzung zum Recht des Zugänglichmachens wird hier vom Anbieter festgelegt, zu welchem Zeitpunkt eine Übertragung beginnt.<sup>178</sup>

<sup>174</sup> PFORTMÜLLER, SHK URG, Art. 11 N 10; BARRELET/EGLOFF, Art. 10 N 26 f.; REHBINDER/VIGANÒ, Art. 10 N 18.

<sup>175</sup> BARRELET/EGLOFF, Art. 10 N 26 f.; BRÄNDLI/TAMÒ, sic! 2013, 655 f.; HILTY, Urheberrecht, Rz. 173.

<sup>176</sup> WIGGER/KORRODI, sic! 2013, 470 f., m.w.H.; HILTY, Urheberrecht, Rz. 173 und 177; REHBINDER/VIGANÒ, Art. 10 N 20; BARRELET/EGLOFF, Art. 10 N 7a und N 22a; a.A. GLARNER, Musikpiraterie im Internet, 123 f. und BÜHLER, 200 f., die für eine Subsumtion unter Art. 10 Abs. 2 lit. c URG plädieren.

<sup>177</sup> DESSEMONTET, SIWR II/1, 202 ff.; BARRELET/EGLOFF, Art. 10 N 24; HILTY, Urheberrecht, Rz. 177.

<sup>178</sup> BRÄNDLI/TAMÒ, sic! 2013, 655; PFORTMÜLLER, SHK URG, Art. 10 N 11; BARRELET/EGLOFF, Art. 10 N 26; REHBINDER/VIGANÒ, Art. 10 N 20.

### **A. Nicht-lineares Streaming**

- 56 Da der einzelne Nutzer beim nicht-linearen Streaming selbst – durch individuellen Abruf – über den Zeitpunkt der Werkwiedergabe bestimmt, ist das in Art. 10 Abs. 2 lit. d URG statuierte Senderecht nicht tangiert.<sup>179</sup>

### **B. Lineares Streaming**

- 57 Das Senderecht ist sowohl beim Live-Streaming, beim Near-On-Demand-Streaming wie auch bei sämtlichen Streaming-Verfahren, in denen nicht der Nutzer, sondern der Stream-Anbieter über den Programmablauf bestimmt und derselbe Inhalt zeitgleich an eine unbestimmte Vielzahl von Personen gesendet wird, einschlägig.<sup>180</sup> Das Live-Streaming bildet das „Internet-Äquivalent zum klassischen Rundfunk“<sup>181</sup>. Aufgrund des festen Sendepfandes ist auch das Near-on-Demand-Streaming im Bereich des Rundfunks anzusiedeln und unter das Senderecht zu subsumieren.<sup>182</sup> Folglich muss ein Stream-Anbieter sowohl für das Live-Streaming als auch das Near-on-Demand-Streaming von urheberrechtlich geschützten Werken vorgängig das Senderecht nach Art. 10 Abs. 2 lit. d URG von den Rechteinhabern einholen.

## **4. Werkintegrität (Art. 11 URG)**

- 58 Das in Art. 11 URG geregelte Bearbeitungsrecht bezweckt den Schutz der Werkintegrität.<sup>183</sup> Eine bloss technische Umwandlung eines Werks ist nicht

---

<sup>179</sup> BRÄNDLI/TAMÒ, sic! 2013, 655 f.; PFORTMÜLLER, SHK URG, Art. 10 N 11; HILTY, Urheberrecht, Rz. 173 und 177; JOLLER, 123; BARRELET/EGLOFF, Art. 10 N 26.

<sup>180</sup> BRÄNDLI/TAMÒ, sic! 2013, 656; JOLLER, 123; AUF DER MAUR, SHK URG, Art. 33 N 20; GILLIÉRON, sic! 2009, 757; BU, 57 und 119; a.A. GLARNER, Musikpiraterie im Internet, 123, der das Senderecht nicht tangiert sieht, weil das Werk nicht „an eine unbestimmte Anzahl von Personen, sondern zielgerichtet und ausschliesslich an jene Empfänger erfolgt, welche das Angebot aktiv abrufen“; BARRELET/EGLOFF, Art. 10 N 26a, die das Live-Streaming als Wahrnehmbarmachung i.S.v. Art. 10 Abs. 2 lit. c URG qualifizieren; BÜHLER, 200 f.; zum deutschen Recht vgl. VON APPEN/BARATH, CaS 2014, 248 f.; EICHELBERGER, 24; VON GERLACH, 51; SPINDLER, FS-Weber, 796 ff.; RADMANN, ZUM 2010, 388 f.; BÜSCHER/MÜLLER, GRUR 2009, 558 f.

<sup>181</sup> STOLZ, MMR 2013, 354.

<sup>182</sup> BRÄNDLI/TAMÒ, sic! 2013, 656, m.w.H.; JOLLER, 123; BU, 57 und 119; RADMANN, ZUM 2010, 388; VON GERLACH, 52.

<sup>183</sup> DESSEMONTET, SIWR II/1, 206 ff.; vgl. auch RIGAMONTI, Urheberpersönlichkeitsrechte, 279 ff., m.w.H.; BOSSHART, 92 f.; HILTY, Urheberrecht, Rz. 198.

als Werkänderung zu qualifizieren.<sup>184</sup> Da sich die Werkänderung beim Streaming von Audio-/Video-Dateien auf technische Umwandlungen beschränkt, ist ein Eingriff in die Integrität des Werks zu verneinen. Diskutabel wäre etwa die Annahme eines Eingriffs in die Werkintegrität in Fällen, in denen Bannerwerbung direkt im Wiedergabefenster der gestreamten Audio-/Video-Datei eingebunden wird.<sup>185</sup>

## 5. Erschöpfungsgrundsatz (Art. 12 URG)

### A. Allgemeines

Der in Art. 12 URG verankerte Erschöpfungsgrundsatz besagt, dass sich das ausschliessliche Verbreitungsrecht des Urhebers an einem Werkexemplar mit dessen erstmaliger Veräusserung erschöpft.<sup>186</sup> Eine nachfolgende Weiterveräusserung durch den Ersterwerber fällt deshalb nicht mehr unter das Verbreitungsrecht des Urhebers.<sup>187</sup> Die Erschöpfung beschränkt sich dabei auf das Recht, über die weitere Verbreitung des Werks bestimmen zu können.<sup>188</sup> Sämtliche übrigen Rechte des Urhebers am betreffenden Werk bleiben indessen bestehen.<sup>189</sup> Ziel des Erschöpfungsgrundsatzes ist es, die freie Zirkulation der in Umlauf gesetzten Werkexemplare zu gewährleisten.<sup>190</sup>

---

<sup>184</sup> BARRELET/EGLOFF, Art. 11 N 6a; GLARNER, Musikpiraterie im Internet, 98 f.; BÜHLER, 158, 218 f.; strenger PFORTMÜLLER, SHK URG, Art. 11 N 3, der bereits Umformatierungen eines Werks vom Schutzbereich erfasst sieht, sofern diese mit qualitativen Unterschieden verbunden sind.

<sup>185</sup> FUCHS/FARKAS, ZUM 2015, 121 f., bejahen eine Entstellung des Werks, bei einer Einrahmung in Werbung für Erotikseiten; vgl. zum deutschen Recht BRUNOTTE, 37 f., der eine Entstellung des Werks für denkbar hält, falls die Komprimierung des Filmwerks nicht den technischen Umständen bei der Übertragung geschuldet ist und dazu ein Ausmass erreicht, so dass die berechtigten Interessen des Urhebers tangiert sind.

<sup>186</sup> BÖTTCHER, 32; PFORTMÜLLER, SHK URG, Art. 12 N 1.

<sup>187</sup> HILTY, Urheberrecht, Rz. 160; PFORTMÜLLER, SHK URG, Art. 12 N 4, mit dem Hinweis, dass ein einmal veräussertes Werkexemplar nicht nur weiterveräussert, sondern auch „sonstwie verbreitet“ werden darf.

<sup>188</sup> PFORTMÜLLER, SHK URG, Art. 12 N 1; BARRELET/EGLOFF, Art. 12 N 9 ff.

<sup>189</sup> PFORTMÜLLER, SHK URG, Art. 12 N 1; BARRELET/EGLOFF, Art. 12 N 9 ff.; REHBINDER, Urheberrecht, 134 ff.

<sup>190</sup> BÖTTCHER, 227; NEFF/ARN, SIWR II/2, 245.

## **B. Der Erschöpfungsgrundsatz im digitalen Umfeld**

- 60 Die Anwendung des Erschöpfungsgrundsatzes setzt gem. Art. 12 URG eine Veräußerung des Werks durch die Urheberschaft bzw. deren Zustimmung zur Veräußerung voraus. Unter den Begriff der Veräußerung fallen sämtliche Formen der Übereignung wie der Verkauf, der Tausch oder die Schenkung, nicht aber die Leihe oder die Vermietung.<sup>191</sup>
- 61 Die Frage, ob sich der Erschöpfungsgrundsatz nur auf körperliche Werke bezieht oder ob auch unkörperliche (digitale) Werke mitumfasst sind, wird in der Lehre kontrovers diskutiert.<sup>192</sup> Gewisse Autoren lehnen eine Unterscheidung zwischen der Veräußerung körperlicher und unkörperlicher Werkexemplare ab und erklären den Erschöpfungsgrundsatz auch bei der Veräußerung unkörperlicher Werke für anwendbar.<sup>193</sup> Andere Autoren wollen den Begriff „Werkexemplare“ eng auslegen und sehen nur körperliche Werke erfasst.<sup>194</sup> Eine solche Einschränkung des Erschöpfungsgrundsatzes ist m.E. abzulehnen, denn sie widerspricht der ratio legis, wonach der Erschöpfungsgrundsatz eine möglichst weitgehende Verkehrsfähigkeit eines Werks sicherstellen soll.<sup>195</sup> Nach HILTY ist Art. 12 Abs. 1 URG dahingehend auszulegen, „dass der rechtmässige Onlineerwerb von Werken und deren (ebenfalls rechtmässige) Fixierung auf einem Datenträger durch den Onlineerwerber mit Bezug auf diesen Datenträger entsprechend der Konstellation der Veräußerung eines Werkexemplars im Sinne jener Norm zu behandeln ist“<sup>196</sup>. Zustimmend mit BÖTTCHER sollte für die Annahme einer Veräußerungshandlung nicht die Art der Distribution (etwa durch Überlassung eines physischen Datenträgers oder rein elektronisch mit-

---

<sup>191</sup> PFORTMÜLLER, SHK URG, Art. 12 N 3; BARRELET/EGLOFF, Art. 12 N 9 ff.; REHBINDER/VIGANÒ, Art. 12 N 1.

<sup>192</sup> BÖTTCHER, 141, m.w.H.; HILTY, Urheberrecht, Rz. 162; RIGAMONTI, GRUR-Int. 2009, 19; SCHACK, GRUR 2007, 644; soweit ersichtlich, wurde diese Frage bislang von der schweizerischen Rechtsprechung noch nicht behandelt.

<sup>193</sup> BÖTTCHER, 140 ff., der zudem zwischen analogen Werken in digitalisierter Form und originär digitalen Werken differenziert; PFORTMÜLLER, SHK URG, Art. 12 N 10; HILTY, Urheberrecht, Rz. 162; REHBINDER/VIGANÒ, Art. 12 N 2, bejahen den Eintritt der Erschöpfung soweit „die Bereitstellung eines Datensatzes zum *Download* als Substitut für den Erwerb einer physischen Kopie konzipiert ist“; BÜHLER, 275 ff.; NEFF/ARN, SIWR II/2, 248.

<sup>194</sup> ARI, 67; SEMADENI, 148 ff.

<sup>195</sup> BÖTTCHER, 190; HILTY, Urheberrecht, Rz. 162.

<sup>196</sup> HILTY, Urheberrecht, Rz. 162.

tels eines Downloads) entscheidend sein, sondern einzig der Umstand, ob der Erwerber dadurch einen dauerhaften Zugriff auf das Werkexemplar erhält.<sup>197</sup>

Da beim Streaming das Werkstück i.d.R. nicht dauerhaft abgespeichert wird, sondern nur transitorische Vervielfältigungen hergestellt werden, erhält der Nutzer keinen dauerhaften Zugriff auf das Werkexemplar.<sup>198</sup> Folglich liegt keine Veräußerungshandlung vor. Falls ein Nutzer durch eine Manipulation der Einstellungen der Abspielsoftware bzw. durch die Verwendung eines Stream-Recorders oder eines Konvertierungsdienstes in den Besitz einer dauerhaften Werkkopie gelangt, erschöpft sich das Verbreitungsrecht an diesem Werkexemplar trotzdem nicht, weil auf das Vertragsverhältnis zwischen dem Rechteinhaber und dem Endnutzer kein Kaufvertragsrecht zur Anwendung kommt.<sup>199</sup>

Da die digitalen Werke meist nur während einer beschränkten Zeitspanne (z.B. während 48 Stunden bei pay-per-view-Angeboten oder während der Vertragsdauer des Abonnements bei flat-rate-Angeboten<sup>200</sup>) konsumiert werden können, ist auf das zugrundeliegende Vertragsverhältnis zwischen den Rechteinhabern und dem Endnutzer das Mietrecht oder die Gebrauchsleihe (bei kostenlosen, werbefinanzierten Angeboten) analog anzuwenden.<sup>201</sup> Gleiches gilt auch für das Streaming von Computerspielen, bei dem die Anbieter den Nutzern während der Laufzeit der Mitgliedschaft einen Online-Zugriff auf Computerspiele gewähren, die sodann mittels Streaming konsumiert werden können.<sup>202</sup>

BÖTTCHER weist zutreffend darauf hin, dass die Zuordnung der Verfügbarmachung digitaler Werke mittels Streaming unter das Verbreitungsrecht gem. Art. 10 Abs. 2 lit. b URG fraglich sei: Da beim Streaming im Regelfall kein Werkexemplar beim Nutzer verbleibt, sei es naheliegender, die Verfügbarmachung

<sup>197</sup> BÖTTCHER, 144 ff.; RIGAMONTI, AJP 2010, 585 f.; BERGER, GRUR 2002, 201; einschränkend, BARRELET/EGLOFF, Art. 12 N 1a, nach deren Ansicht die Erschöpfung nur dann eintreten kann, wenn im Anschluss an die Übermittlung in digitaler Weise ein körperliches Werkexemplar hergestellt wird; a.A. ARI, 67; SEMADENI, 148 ff.

<sup>198</sup> Ebenso BÖTTCHER, 216 f.

<sup>199</sup> BÖTTCHER, 217.

<sup>200</sup> Häufig werden die Abonnemente monatlich gelöst, so z.B. bei Netflix, Spotify, OnLive (Service eingestellt am 30. April 2015) oder Apple Music.

<sup>201</sup> Eine bloss analoge Anwendung des Mietrechts nach Art. 253 ff. OR drängt sich deshalb auf, weil der Wortlaut der Bestimmung von „Sache“ spricht, worunter nur körperliche Gegenstände zu subsumieren sind; vgl. auch BÖTTCHER, 217, der das Werkvertrags- bzw. Mietrecht für einschlägig hält.

<sup>202</sup> Vgl. dazu Rz. 32 f.; es liegt keine Veräußerungshandlung i.S.v. Art. 12 Abs. 2 URG vor.

chung mittels Streaming unter das Recht der öffentlichen Zugänglichmachung nach Art. 10 Abs. 2 lit. c URG zu subsumieren, mit der Konsequenz, dass sich die Frage nach der Erschöpfung nicht stellt, da diese nur bei Veräusserungshandlungen einschlägig ist.<sup>203</sup>

- <sup>65</sup> Gewisse Anbieter bieten für sog. Premium-Kunden den Service an, dass einzelne Musikstücke auch auf das Endgerät des Nutzers heruntergeladen werden können.<sup>204</sup> Ungeachtet dessen liegt auch in diesen Fallkonstellationen keine Veräusserungshandlung i.S.v. Art. 12 Abs. 1 URG vor, da der Werkzugriff und die Werknutzung durch technische Massnahmen eingeschränkt wird. Konkret werden die Werke so geschützt, dass sie weder vervielfältigt noch weiterverbreitet werden können und nach Ablauf der Vertragsdauer des Abonnements, automatisch gelöscht werden. Die Überlassung der Werke ist also von vornherein bloss vorübergehender Natur.<sup>205</sup>

## 6. Zwischenergebnis

- <sup>66</sup> Die bisherige Untersuchung hat gezeigt, dass die Frage nach den für die Werkverwertung mittels Streaming erforderlichen Verwertungsrechten, nicht einheitlich beantwortet werden kann. Es muss stets zwischen den verschiedenen Streaming-Verfahren differenziert werden:
- Beim nicht-linearen On-Demand-Streaming wie auch beim linearen Near-On-Demand-Streaming müssen die Stream-Anbieter von den Rechteinhabern das Vervielfältigungsrecht nach Art. 10 Abs. 2 lit. a URG einholen, weil hier – technisch bedingt – eine vorgängige körperliche Fixierung des Werks auf einem *Server* vorausgesetzt ist.
  - Auch das lineare Live-Streaming tangiert das Vervielfältigungsrecht nach Art. 10 Abs. 2 lit. a URG, da zur Verbreitung des Werks sukzes-

---

<sup>203</sup> Zum Ganzen BÖTTCHER, 217; siehe auch PFORTMÜLLER, SHK URG, Art. 12 N 3; GLARNER, Musikpiraterie im Internet, 155.

<sup>204</sup> <<https://www.spotify.com/ch-de/premium>> (besucht 25. August 2015); dadurch können die Werke auch offline auf mobilen Endgeräten genutzt werden.

<sup>205</sup> BÖTTCHER, 217; PFORTMÜLLER, SHK URG, Art. 12 N 3, „ob eine Veräusserung vorliegt, entscheidet nicht in erster Linie die Benennung des Vertrages, vielmehr ist eine, auch wirtschaftliche Gesichtspunkte einbeziehende, Gesamtbetrachtung vorzunehmen“; BARRELET/EGLOFF, Art. 12 N 9.



sive ephemere Vervielfältigungen von Werkteilen auf den *Servern* der Anbieter hergestellt werden.<sup>206</sup>

- Da beim nicht-linearen On-Demand-Streaming die Nutzer über den Zeitpunkt der Wiedergabe des Werks bestimmen, haben die Stream-Anbieter von den Rechteinhabern das Recht der Zugänglichmachung nach Art. 10 Abs. 2 lit. c URG einzuholen.
- Demgegenüber beschlagen die linearen Streaming-Verfahren (Live-Streaming, Near-on-Demand-Streaming) das Recht der öffentlichen Zugänglichmachung nach Art. 10 Abs. 2 lit. c URG nicht, da hier die Anbieter über den Zeitpunkt der Werkwiedergabe bestimmen.
- Im Unterschied zum nicht-linearen On-Demand-Streaming ist bei sämtlichen linearen Streaming-Verfahren das Senderecht nach Art. 10 Abs. 2 lit. d URG tangiert, weil hier der Anbieter festlegt, wann die Werkwiedergabe beginnt und derselbe Inhalt zeitgleich an eine beliebige Anzahl von Nutzern gesendet wird.

Falls ein Stream-Anbieter unerlaubt urheberrechtlich geschützte Werke auf dem Wege des Streaming verwertet, können die Rechteinhaber gegen die Urheberrechtsverletzung einen Strafantrag nach Art. 67 URG (bzw. nach Art. 69 URG) stellen. Zivilrechtlich können die Rechteinhaber auf Feststellung der Rechtsverletzung (Art. 61 URG), auf Unterlassung oder Beseitigung der Urheberrechtsverletzung (Art. 62 Abs. 1 lit. a und lit. b URG), sowie auf Schadenersatz<sup>207</sup> für die begangene Urheberrechtsverletzung klagen (Art. 62 Abs. 2 URG). 67

## 7. Sonderfall: *Framing*

### A. Technische Einführung des *Framing*

Im Unterschied zu einem Hyperlink, durch dessen Anklicken der Nutzer entweder auf Unterseiten derselben Webseite (*interner Link*) oder auf eine 68

---

<sup>206</sup> S.o. Rz. 49 f.

<sup>207</sup> Urteil des Obergerichts des Kantons Zug vom 20. Februar 2013, GVP 2013, 169, Erw. 4, „die untere Limite für die Schadenersatzberechnung muss dabei derjenige Betrag sein, den die Klägerin bei erlaubtem Gebrauch des Werks als Vergütung hätte beanspruchen können“; Urteil des Obergerichts Zürich vom 1. Februar 2008, sic! 2008, 630; BAUMGARTNER, 208 f., m.w.H.

andere Webseite (*externer Link*) weitergeleitet wird, werden beim *Framing* digitale Inhalte einer fremden Webseite direkt in einem abgegrenzten Bereich auf der Webseite des verweisenden Betreibers eingebunden (*Inline-Framing*) oder in einem neuen Fenster (*Pop-up*) angezeigt.<sup>208</sup> Dadurch können fremde Medieninhalte als komplett integrierter Teil auf einer beliebigen Webseite wiedergegeben werden, „obwohl die Datei auf einer fremden Webseite, also einem anderen *Server* liegt“<sup>209</sup>. Der Linksetzer bzw. diejenige Person, welche fremde Medieninhalte mittels *Inline-Framing* in eine andere Webseite einbettet, hat selbst keine Kontrolle über die verlinkten bzw. geframten Inhalte.<sup>210</sup>

## **B. Rechtliche Qualifikation des *Framing***

### **a) *Vervielfältigungsrecht***

- <sup>69</sup> Beim *Framing* findet keine Vervielfältigung des Werks auf den *Servern* des verweisenden Betreibers statt.<sup>211</sup> Obschon das Werk direkt auf der verweisenden Webseite abgerufen werden kann, ist es weiterhin nur auf den *Servern* der verlinkten (fremden) Webseite abgespeichert, weshalb das Vervielfältigungsrecht nach Art. 10 Abs. 1 lit. a URG nicht tangiert ist.<sup>212</sup>

---

<sup>208</sup> VOLZ, 168, spricht diesbezüglich von einer „Verschmelzung verschiedener Website-Inhalte“; AREZZO, IIC 2014, 524 ff.; REUSSER, 16 ff.; DRAHEIM/LEHMANN, GRUR-Prax 2014, 427; HENDEL, ZUM 2014, 102; BÄCKER/HÖFINGER, ZUM 2013, 627 f.; EISELE, 224; WEBER, E-Commerce, 229; HOEREN, MMR 2004, 645; SCHWARZENEGGER/NIGGLI, medialex 2003, 27; GILLIÉRON, sic! 2000, 756.

<sup>209</sup> HENDEL, ZUM 2014, 102; LEISTNER, GRUR 2014, 1154; BÄCKER/HÖFINGER, ZUM 2013, 627 f.; ULLRICH, ZUM 2010, 853, weist darauf hin, dass sowohl On-Demand-Streams wie auch Live-Streaming-Angebote mittels der *Framing*-Technik in eine Webseite eingebunden werden können; FANGEROW/SCHULZ, GRUR 2010, 678.

<sup>210</sup> FUCHS/FARKAS, ZUM 2015, 110.

<sup>211</sup> FUCHS/FARKAS, ZUM 2015, 110 f.; HENDEL, ZUM 2014, 106; SCHAPIRO/JENSSEN, ZUM 2013, 665.

<sup>212</sup> FUCHS/FARKAS, ZUM 2015, 110 f., m.w.H.; BRUNOTTE, 46, weist darauf hin, dass das Videomaterial des *embedded Players* zu keinem Zeitpunkt auf dem *Server* desjenigen abgelegt wird, der den Player im Rahmen seines Internetangebots auf seiner Webseite einbindet; OTT, ZUM 2004, 361.

### b) Öffentliche Zugänglichmachung

Eine Besonderheit beim *Framing* liegt darin, dass die eingebundenen Inhalte (*embedded content*) bereits auf einer anderen Webseite zugänglich sind.<sup>213</sup> Es stellt sich deshalb die Frage, ob das Framing als öffentliches Zugänglichmachen i.S.v. Art. 10 Abs. 2 lit. c URG zu qualifizieren ist. Da die letztgenannte Norm und die einschlägige Bestimmung zur Regelung der öffentlichen Wiedergabe nach EU-Recht miteinander vergleichbar sind, wird nachfolgend die Rechtsprechung des EuGH zur Beantwortung dieser Frage herangezogen.

Im *Svensson*-Entscheid anerkannte der EuGH, dass es zulässig ist, mittels Hyperlinks auf frei zugängliche, urheberrechtlich geschützte Werke zu verweisen, ohne dass hierfür vorgängig eine Einwilligung der Rechteinhaber eingeholt werden muss.<sup>214</sup> Der EuGH stellt bei der Beurteilung, ob eine öffentliche Wiedergabe i.S.v. Art. 3 Abs. 1 der Info-Richtlinie vorliegt, schwergewichtig darauf ab, ob sich die Wiedergabe „an ein neues Publikum richtet, d.h. an ein Publikum, das die Inhaber des Urheberrechts nicht hatten erfassen wollen, als sie die ursprüngliche öffentliche Wiedergabe erlaubten“<sup>215</sup>. Wird ein Werk ohne Beschränkung<sup>216</sup> des Zugriffs im Internet veröffentlicht, sei dieses bereits allen Internetnutzern zugänglich gemacht worden, weshalb der Kreis potentieller Adressaten nicht erweitert wird, wenn „die betreffenden Werke über einen anklickbaren Link [...] zugänglich gemacht werden [...]“<sup>217, 218</sup>. Sodann präziserte der EuGH, dass seine Beurteilung selbst dann nicht in Frage gestellt werden könne, wenn das Werk bei Abruf des fraglichen Links durch die Nutzer „in einer Art und Weise erscheint, die den Eindruck vermittelt, dass es auf der Seite erscheint, auf der sich dieser Link befindet, obwohl es [das Werk] in Wirklichkeit einer anderen Seite

<sup>213</sup> HENDEL, ZUM 2014, 102; WEIL, sic! 2014, 481 f., m.w.H.; REUSSER, Jusletter vom 28. April 2014, Rz. 4; OTT, ZUM 2004, 362.

<sup>214</sup> EuGH vom 13. Februar 2014, Rechtssache C-466/12, *Svensson*, Rz. 29 f.; vgl. auch KAEMPF/BÜRGE, 238.

<sup>215</sup> EuGH vom 13. Februar 2014, Rechtssache C-466/12, *Svensson*, Rz. 24.

<sup>216</sup> Vgl. EuGH vom 13. Februar 2014, Rechtssache C-466/12, *Svensson*, Rz. 31., etwa durch Zugangsschranken.

<sup>217</sup> EuGH vom 13. Februar 2014, Rechtssache C-466/12, *Svensson*, Rz. 25.

<sup>218</sup> VON UNGERN-STERNBERG, GRUR 2015, 209; SPINDLER, NJW 2014, 2550; LEISTNER, GRUR 2014, 1152; KAEMPF/BÜRGE, 238; a.A. HÖFINGER, ZUM 2014, 294; REUSSER, 62; HENDEL, ZUM 2014, 105 f., der ein neues Publikum annimmt, sobald ein Werk in eine neue digitale Umgebung gebracht wird und zusammen mit anderen Werken gesammelt, kategorisiert oder auch bloss leichter zugänglich gemacht wird.

entstammt“<sup>219</sup>. In der *BestWater*-Entscheidung hat der EuGH diese Rechtsprechung mit Blick auf die *Framing*-Technik bestätigt.<sup>220</sup>

- 72 An der Rechtsprechung des EuGH wurde u.a. kritisiert, dass ein Hyperlink nicht als bloße Fussnote zu bewerten sei, die lediglich das Auffinden digitaler Inhalte im Internet erleichtern würde.<sup>221</sup> Insbesondere wird eingewendet, dass diese Beurteilung jene Fälle ausser Betracht lässt, bei denen ein bestimmter Inhalt überhaupt erst durch das Setzen des Hyperlinks auffindbar gemacht wird.<sup>222</sup> Ferner stösst die weite Auslegung des Begriffs der „Öffentlichkeit“ auf Kritik: Der Rechteinhaber habe nur der Veröffentlichung seines Werks hinsichtlich der ursprünglichen Webseite zugestimmt und dabei nur die Nutzer dieser Webseite als Publikum in Betracht gezogen.<sup>223</sup> HENDEL ist der Ansicht, dass ein „neues Publikum“ auch dann vorliegen würde, falls „die Öffentlichkeit auf anderem Weg überhaupt nicht oder nur mit erheblichem Mehraufwand – also insbesondere nicht über die üblichen Suchmaschinen – zur Darstellung des geschützten Werkes gelangen kann“<sup>224</sup>.
- 73 Letztgenannter Lösungsansatz lässt sich m.E. nur schwer mit dem öffentlichen Interesse an einem möglichst ungehinderten Zugang zu Informationen

---

<sup>219</sup> EuGH vom 13. Februar 2014, Rechtssache C-466/12, *Svensson*, Rz. 29 f.; siehe WILLE, GRUR-Prax 2014, 331; JANI/LEENEN, GRUR 2014, 362; KAEMPF/BÜRGE, 238; WEIL, sic! 2014, 481 f.

<sup>220</sup> EuGH vom 21. Oktober 2014, Rechtssache C-348/13, *BestWater International*, Rz. 19, wonach die Einbettung eines auf einer Webseite öffentlich zugänglichen geschützten Werkes in eine andere Webseite mittels eines Links unter Verwendung der *Framing*-Technik, keine öffentliche Wiedergabe i.S.v. Art. 3 Abs. 1 der Info-Richtlinie darstellt, „soweit das betreffende Werk weder für ein neues Publikum noch nach einem speziellen technischen Verfahren wiedergegeben wird, das sich von demjenigen der ursprünglichen Wiedergabe unterscheidet.“

<sup>221</sup> REUSSER, Jusletter vom 28. April 2014, Rz. 4; HENDEL, ZUM 2014, 104, nach dessen Ansicht ein *Deep-Link* eine andere Qualität als rein informierende Fussnoten aufweisen würde; a.A. SCHMIDT-WUDY, EuZW 2014, 268;

<sup>222</sup> HÖFINGER, ZUM 2014, 293, wenn das Werk zuvor auf einem *Filehoster* veröffentlicht wurde, jedoch erst durch die Veröffentlichung des *Links* für das Publikum zugänglich gemacht wird.

<sup>223</sup> SCHULZE, ZUM 2015, 110; HÖFINGER, ZUM 2014, 294; WEIL, sic! 2014, 482; HENDEL, ZUM 2014, 105 f.

<sup>224</sup> HENDEL, ZUM 2014, 105, plädiert weiter dafür, dass der Tatbestand der Zugänglichmachung umso leichter als erfüllt angesehen werden sollte, „je grösser die neue Öffentlichkeit ist, die erst durch den *Link* zu der Darstellung gelangen kann“; ähnlich ULLRICH, ZUM 2010, 857 f.

vereinbaren.<sup>225</sup> Aufgrund der Globalität des Internets sollte vielmehr von der Prämisse ausgegangen werden, dass diejenige Person, welche einen Inhalt über das Internet zugänglich macht und dabei auf den Einsatz technischer Massnahmen zur Beschränkung der potentiellen Empfänger verzichtet, konkludent dazu einwilligt, dass der Inhalt auch mittels *Framing*-Technik in eine andere Webseite eingebettet werden darf.<sup>226</sup>

Nach hier vertretener Auffassung lässt sich die Rechtsprechung des EuGH auch auf das Schweizer Recht übertragen und folglich sollte das Vorliegen einer öffentlichen Zugänglichmachung erst dann bejaht werden, wenn das Werk gegenüber einem neuen Publikum zugänglich gemacht wird.<sup>227</sup> Ein neues Publikum soll dann vorliegen, wenn den Nutzern durch den Einsatz von *Links* oder *Frames* ermöglicht wird, „beschränkende Massnahmen zu umgehen, die auf der Seite, auf der das geschützte Werk zu finden ist, getroffen wurden, um den Zugang der Öffentlichkeit [...] zu beschränken“<sup>228</sup>. Richtigerweise sind darunter nicht nur Zugangsschranken (etwa *pay-walls*) zu subsumieren, sondern sämtliche technischen Schutz- und Steuerungsmöglichkeiten, die dazu geeignet und bestimmt sind, die *Verlinkung* bzw. das *Framing* von urheberrechtlich geschützten Werken wirksam zu verhindern (Nutzungsschranken).<sup>229</sup>

Sofern die Rechteinhaber den Zugang zum Werk oder dessen Verlinkung durch wirksame technische Massnahmen beschränken, darf dieses – ohne Einwilligung – nicht mittels *Framing* auf einer anderen Webseite zugänglich gemacht werden. Andernfalls liegt eine unrechtmässige öffentliche Zugänglichmachung nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG vor. In solchen Fallkonstellationen, in denen vorab eine wirksame technische Massnahme umgangen werden muss, um das Werk mittels *Framing* auf einer anderen Webseite

<sup>225</sup> FUCHS/FARKAS, ZUM 2015, 110 f., weisen darauf hin, dass *Hyperlinks* ein wesentlicher Bestandteil des Internets und der Kommunikationsgesellschaft sind.

<sup>226</sup> Vgl. EuGH vom 21. Oktober 2014, Rechtssache C-348/13, BestWater International, Rz. 18; a.A. HENDEL, ZUM 2014, 110, ist der Meinung, dass aus dem Umstand, dass ein Rechteinhaber sein Werk über das Internet zugänglich macht, nicht ohne Weiteres abgeleitet werden könne, dass er in jede Form der *Verlinkung* eingewilligt habe.

<sup>227</sup> EuGH vom 21. Oktober 2014, Rechtssache C-348/13, BestWater International, Rz. 18 f.

<sup>228</sup> EuGH vom 13. Februar 2014, Rechtssache C-466/12, Svensson, Rz. 31.

<sup>229</sup> VON UNGERN-STERMBERG, GRUR 2015, 209; AREZZO, IIC 2014, 543; HENDEL, ZUM 2014, 110, verweist auf die Möglichkeit, bereits bei der Programmierung der Webseite die Möglichkeit der *Verlinkung* der Dateien teilweise oder vollständig zu unterbinden. Auf der Streaming-Plattform YouTube lässt sich die *Verlinkung* der hochgeladenen Inhalte durch das Setzen eines entsprechenden Häkchens beim *Upload* verhindern.

einbinden zu können, liegt zudem regelmässig eine Umgehung einer technischen Massnahme zum Zwecke einer gesetzlich unerlaubten Verwendung von Werken vor (Art. 69a Abs. 1 lit. a URG). Die Rechtswidrigkeit der Verwendung liegt in der unrechtmässigen Zugänglichmachung des Werks auf der verweisenden Webseite, auf der das Werk zum Abruf durch Dritte bereitgehalten wird.

- 76 HÖFINGER beanstandet an der Auslegung des EuGH, dass die Rechteinhaber nicht gegen Personen vorgehen können, die auf rechtswidrig zugänglich gemachte Werke *verlinken*.<sup>230</sup> HENDEL ist der Ansicht, dass in Fällen, in denen der erste *Upload* ohne Zustimmung der Rechteinhaber erfolgt ist, die *Verlinkung per se* rechtswidrig sei.<sup>231</sup> GLARNER vertritt die Auffassung, dass sich der *Link-Setzer* die unerlaubten Inhalte zu eigen machen will, wenn er diese dergestalt in seine Webseite integriert, dass sie als Bestandteil derselben erscheinen. Deshalb sei der *Link-Setzende* in diesem Fall als Haupttäter zu bestrafen.<sup>232</sup>
- 77 Im Unterschied zur *Verlinkung* von rassistischen oder kinderpornografischen Inhalten (Art. 261<sup>bis</sup> StGB bzw. Art. 197 Abs. 4 StGB), deren Rechtswidrigkeit sich durch das bloss Betrachten meist eindeutig erschliessen lassen, wird ein *Link-Setzer* bei urheberrechtswidrig zugänglich gemachten Inhalten nur selten klar beurteilen können, ob bei der ursprünglichen Zugänglichmachung des Werks sämtliche Einwilligungen von den Rechteinhabern eingeholt worden sind.<sup>233</sup>
- 78 Nach hier vertretener Ansicht ist es für den *Linksetzer* nicht zumutbar, wenn er vor der Verlinkung eines Werks in Erfahrung bringen muss, ob der ursprüngliche *Upload* mit Einwilligung der Rechteinhaber erfolgt war.<sup>234</sup> Die Rechteinhaber sind auch in diesen Fällen nicht schutzlos. Es verbleibt ihnen

---

<sup>230</sup> HÖFINGER, ZUM 2014, 295.

<sup>231</sup> HENDEL, ZUM 2014, 110.

<sup>232</sup> GLARNER, Musikpiraterie im Internet, 146.

<sup>233</sup> Gl. M. VON UNGERN-STERMBERG, GRUR 2015, 209 f., der darauf hinweist, dass es nicht Sinn der Rechtsprechung des EuGH sein kann, *Linksetzer* einem unkalkulierbaren Risiko auszusetzen; WEBER, E-Commerce, 556; SCHWARZENEGGER/NIGGLI, medialex 2003, 29 f.; SCHWARZENEGGER, NZZ, 71.

<sup>234</sup> VON UNGERN-STERMBERG, GRUR 2015, 210, führt dazu aus, dass wer gutgläubig einen *Hyperlink* auf eine fremde Webseite setzt, in aller Regel nicht pflichtwidrig oder zumindest nicht schuldhaft handelt; a.A. HENDEL, ZUM 2014, 111, der es für zumutbar hält, dass die *Link-Provider* vor der Einbettung eines Werks in Erfahrung bringen, ob die Rechteinhaber mit der konkreten Nutzung einverstanden sind.

stets die Möglichkeit, den Betreibern der Webseite auf der sich der *Link* bzw. *Frame* befindet, mitzuteilen, dass das *verlinkte* Werk ohne deren Einwilligung hochgeladen wurde und der *Frame* deshalb von der Webseite zu entfernen sei. Falls die Betreiber der Webseite dieser Löschaufforderung nicht Folge leistet, kommt eine Gehilfenschaft zu einer unerlaubten Zugänglichmachung nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG i.V.m. Art. 25 StGB in Betracht.<sup>235</sup>

Das Bundesgericht musste bisher noch keine urheberrechtliche Bewertung von *Hyperlinks* oder zum *Framing* vornehmen.<sup>236</sup> Da die Entscheide des EuGH für die Schweizer Gerichte keine bindende Wirkung zeitigen, bleibt abzuwarten, wie diese in einem solchen Fall entscheiden werden.<sup>237</sup> 79

## II. Illegale Streaming-Dienste (am Beispiel von *kino.to*)

### 1. Übersicht

Auf der Webseite *kino.to* wurde – ohne Einwilligung der Rechteinhaber – eine umfangreiche *Linksammlung* zu einer Vielzahl urheberrechtlich geschützter Filmwerke angeboten.<sup>238</sup> Zu diesem Zweck rekrutierten die Mitarbeiter von *kino.to* sog. *Uploader*, welche die geschützten Werke aus Deutschland (Leipzig) auf ausländische *Server* (zunächst in den Niederlanden, anschliessend in Russland) hochluden.<sup>239</sup> Die *Filehoster*, auf deren *Server* die Werke abgespeichert wurden, bewarben sich ebenfalls für die Zusammenarbeit mit *kino.to*.<sup>240</sup> Die Mitarbeiter von *kino.to* prüften die von den *Uploadern* hochgeladenen *Links* auf die Einhaltung inhaltlicher Vorgaben 80

---

<sup>235</sup> REHBINDER/VIGANÒ, Art. 67 N 14.

<sup>236</sup> WEIL, sic! 2014, 482.

<sup>237</sup> WEIL, sic! 2014, 482, verweist zutreffend auf die Vergleichbarkeit des schweizerischen Rechts mit dem EU-Recht und folgert daraus, dass auch in der Schweiz eine grundsätzliche Zulässigkeit der Hyperlinks erwartet werden kann.

<sup>238</sup> Nach dem gleichen Prinzip funktionieren auch die nachempfundenen Seiten kinox.to, kinox.tv und kinox.me; STOLZ, MMR 2013, 353; SCHÄUFELE, 156 f.; VON GERLACH, 181.

<sup>239</sup> REINBACHER, NStZ 2014, 58; EICHELBERGER, 17.

<sup>240</sup> REINBACHER, NStZ 2014, 58; weist darauf hin, dass sich *kino.to* zumindest teilweise auch selbst als *Filehoster* betätigte.

sowie deren Funktionalität.<sup>241</sup> Sofern bestimmte Vorgaben eingehalten worden waren, wurden die *Links* auf der Webseite von *kino.to* aufgeschaltet. Zuvor waren die Werke für die Öffentlichkeit nicht erreichbar. Erst nach erfolgter Freischaltung der *Links* auf der Webseite von *kino.to* war der Zugriff auf die hochgeladenen Inhalte möglich. Die Nutzer konnten die Webseite von *kino.to* nach den gewünschten Inhalten durchsuchen und diese – durch Abruf der entsprechenden Zieladresse – mittels On-Demand-Streaming konsumieren oder als *Download* dauerhaft auf ihre Rechner herunterladen. Die Betreiber der Webseite von *kino.to* wie auch die externen *Filehoster* erzielten dabei Einnahmen durch das Aufschalten von Werbung auf ihren Plattformen.<sup>242</sup> Die *Filehoster* generierten zudem Einkünfte durch den Verkauf sog. Premium-Abonnements<sup>243</sup>.

- 81 Damit eine urheberstrafrechtliche Bewertung der einzelnen Handlungen nach Schweizer Recht vorgenommen werden kann, wird der Sachverhalt gedanklich dahingehend abgewandelt, als wären sämtliche Handlungen (der *Upload*, das Betreiben der *Linksammlung* und das File-Hosting nicht-lizenzierter Werke) in der Schweiz begangen worden. Sodann beschränkt sich die Bewertung auf das Zugänglichmachen geschützter Werke auf dem Wege des On-Demand-Streaming.

## 2. Strafbarkeit der *Uploader*

### A. Unerlaubte Herstellung von Werkexemplaren

#### a) Objektiver Tatbestand

- 82 Täter kann jede Person sein, die ohne Einwilligung der Rechteinhaber ein urheberrechtlich geschütztes Werk – zum Zwecke einer Verwendung, die ausserhalb des Eigengebrauchs liegt – auf einen *Server* im Internet hochlädt.<sup>244</sup> Eine Berufung auf die Schrankenregelung des Privatgebrauchs nach Art. 19 Abs. 1 lit. a URG ist ausgeschlossen, da die *Uploader* mit der Her-

---

<sup>241</sup> REINBACHER, NStZ 2014, 58, m.w.H.

<sup>242</sup> Zum Ganzen REINBACHER, NStZ 2014, 57, sowie das Urteil des LG Leipzig vom 14. Juni 2012 – KLS 390 Js 191/11, ZUM 2013, 340.

<sup>243</sup> <<http://bitshare.com/premium.html>> (besucht 25. August 2015); die Premium-Abonnements bieten ihren Nutzern zahlreiche Vorteile wie etwa beliebig viele *Downloads* bei maximaler *Download*-Geschwindigkeit ohne Werbung.

<sup>244</sup> BARRELET/EGLOFF, Art. 10 N 12; REHBINDER/VIGANÒ, Art. 10 N 8.



stellung der Werkkopie auf dem *Server* beabsichtigen, diese gegenüber Dritten unerlaubt zugänglich zu machen.<sup>245</sup> Bereits die Übermittlung der *Links* an die Mitarbeiter von *kino.to* fällt nicht mehr unter den Privatgebrauch, da diese nicht zum Kreis eng verbundener Personen i.S.v. Art. 19 Abs. 1 lit. a URG zählen. Ebenso entfällt die Annahme eines Privatgebrauchs, wenn mit der Herstellung von Werkkopien das Erzielen von Einnahmen bezweckt wird.<sup>246</sup> Das Hochladen geschützter Werke zum Zwecke der öffentlichen Zugänglichmachung erfüllt den objektiven Tatbestand von Art. 67 Abs. 1 lit. e URG.

**b) Subjektiver Tatbestand**

Die Erfüllung des subjektiven Tatbestandes setzt voraus, dass die *Uploader* 83 bezüglich sämtlicher objektiver Tatbestandsmerkmale mit Wissen und Wollen gehandelt haben, wobei ein Eventualvorsatz genügt.<sup>247</sup> Vorliegend handelten die *Uploader* in Kenntnis der Unrechtmässigkeit ihrer Handlungen. Das Ziel des gemeinsamen Vorhabens bestand darin, durch die Begehung von Urheberrechtsverletzungen Einkünfte zu erzielen. Die einzelnen (arbeitsteiligen) Vorgänge waren den *Uploadern* bekannt. Durch ihr Verhalten haben die *Uploader* zumindest in Kauf genommen, objektiv tatbestandsmässig zu handeln.

**c) Rechtswidrigkeit und Schuld**

In der vorliegenden Konstellation sind kaum Anwendungsfälle von gesetzli- 84 chen oder übergesetzlichen Rechtfertigungsgründen denkbar. Auch ein Irrtum über die Rechtswidrigkeit nach Art. 21 StGB ist ausgeschlossen, da die *Uploader* die Rechtswidrigkeit ihres Tuns hätten erkennen können und der Irrtum somit nicht unvermeidbar war.<sup>248</sup>

**d) Gewerbsmässiges Handeln**

Falls der Täter für das Hochladen der geschützten Werke eine Vergütung 85 erhält und sich aus der Zeit und den Mitteln, die er für den *Upload* der Wer-

---

<sup>245</sup> S.u. Rz. 199; GASSER, SHK URG, Art. 19 N 8; BÜHLER, 255; GASSER, 64 f.; BARRELET/EGLOFF, Art. 19 N 6 ff.; REHBINDER/VIGANÒ, Art. 19 N 17.

<sup>246</sup> GASSER, SHK URG, Art. 19 N 8; BARRELET/EGLOFF, Art. 19 N 6 ff.; REHBINDER/VIGANÒ, Art. 19 N 17; BÜHLER, 255; GASSER, 64 f.

<sup>247</sup> SCHWARZENEGGER, P2P-Netzwerke, 229; GLARNER, Musikpiraterie im Internet, 87.

<sup>248</sup> DONATSCH/TAG, 222 ff.

ke aufwendet, aus der Häufigkeit der Einzelakte innerhalb eines bestimmten Zeitraums sowie aus den angestrebten und erzielten Einkünften ergibt, dass er das Hochladen von nicht-lizenzierten Werken auf die *Server* der *Filehoster* nach der Art eines Berufs ausübt, ist dieses Handeln als gewerbsmässige Urheberrechtsverletzung nach Art. 67 Abs. 2 URG zu qualifizieren.<sup>249</sup> Die gewerbsmässige Urheberrechtsverletzung gilt als Offizialdelikt und wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.<sup>250</sup>

## **B. Unerlaubte Zugänglichmachung**

### **a) Objektiver Tatbestand**

- 86 Als Täter kommt jede beliebige Person in Frage, die ohne Einwilligung der Rechteinhaber ein geschütztes Werk oder auch bloss Teile davon auf einen *Server* hochlädt und dabei so zugänglich macht, dass Personen von Orten und zu Zeiten ihrer Wahl dazu Zugang haben (Art. 67 Abs. 1 lit. g<sup>bis</sup> URG).<sup>251</sup>

#### *aa) Unrechtmässigkeit der Tathandlung*

- 87 Damit der Tatbestand von Art. 67 Abs. 1 lit. g<sup>bis</sup> URG erfüllt ist, wird ein unrechtmässiges Handeln vorausgesetzt. Gemäss h.L. bildet die Unrechtmässigkeit ein objektives Tatbestandsmerkmal.<sup>252</sup> Liegt eine Einwilligung der Rechteinhaber hinsichtlich der Zugänglichmachung nach Art. 10 Abs. 2 lit. c URG vor, ist eine Tatbestandsmässigkeit nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG ausgeschlossen. Vorliegend fehlt eine entsprechende Einwilligung der Rechtsinhaber.

#### *bb) Rechtmässiger Privatgebrauch*

- 88 Die Unrechtmässigkeit fällt zudem ausser Betracht, wenn die Werkverwendung im Rahmen des Privatgebrauchs nach Art. 19 Abs. 1 lit. a URG stattge-

---

<sup>249</sup> BGE 129 IV 253 Erw. 2.1; 123 IV 113 Erw. 2c; 116 IV 319 Erw. 4; DAVID, SHK URG, Art. 67 N 36, m.w.H.; REHBINDER/VIGANÒ, Art. 67 N 19; KOHLI, sic! 2003, 962 f.

<sup>250</sup> DAVID, SHK URG, Art. 67 N 35; BARRELET/EGLOFF, Art. 67 N 9; REHBINDER/VIGANÒ, Art. 67 N 19.

<sup>251</sup> DAVID, SHK URG, Art. 67 N 20; BARRELET/EGLOFF, Art. 67 N 6a; REHBINDER/VIGANÒ, Art. 67 N 14.

<sup>252</sup> DAVID, SHK URG, Art. 67 N 1a; BARRELET/EGLOFF, Art. 67 N 4; REHBINDER/VIGANÒ, Art. 67 N 4; SCHWARZENEGGER, P2P-Netzwerke, 218 f.; GLARNER, 73 ff.

funden hat. Vorliegend ist zu beachten, dass die *Uploader* die hochgeladenen Werke zunächst nur den Mitarbeitern von *kino.to* zugänglich gemacht haben. Diese zählen jedoch nicht zum Kreis von Personen, die unter sich eng verbunden sind wie Verwandte oder Freunde. Weiter steht der Annahme eines rechtmässigen Eigengebrauchs die Tatsache entgegen, dass die *Uploader* die Erzielung von Einkünften anstreben: Das Erzielen von Einnahmen ist im Rahmen des Privatgebrauchs nach Art. 19 Abs. 1 lit. a URG ausgeschlossen.<sup>253</sup> Der objektive Tatbestand des unerlaubten Zugänglichmachens nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG ist somit erfüllt.

**b) Subjektiver Tatbestand**

Der subjektive Tatbestand von Art. 67 Abs. 1 lit. g<sup>bis</sup> URG setzt ein vorsätzliches Handeln voraus, wobei Eventualvorsatz genügt.<sup>254</sup> Vorliegend wurden die geschützten Werke von den *Uploadern* in Kenntnis um die Rechtswidrigkeit ihrer Handlungen auf die *Server* der *Filehoster* hochgeladen und die entsprechenden URL-Adressen<sup>255</sup> an die Mitarbeiter von *kino.to* übermittelt.<sup>256</sup> 89

**c) Rechtswidrigkeit und Schuld**

Es sind weder gesetzliche noch übergesetzliche Rechtfertigungsgründe denkbar. Auch ein rechtlich beachtlicher Irrtum nach Art. 21 StGB kommt in dieser Konstellation kaum je in Betracht. 90

**d) Gewerbsmässiges Handeln**

Es muss jeweils im konkreten Einzelfall geprüft werden, ob eine gewerbsmässige Begehung einer Urheberrechtsverletzung i.S.v. Art. 67 Abs. 2 URG vorliegt.<sup>257</sup> 91

---

<sup>253</sup> GASSER, SHK URG, Art. 19 N 8; BARRELET/EGLOFF, Art. 19 N 6 ff.; REHBINDER/VIGANÒ, Art. 19 N 17; BÜHLER, 255, GASSER, 64 f.

<sup>254</sup> SCHWARZENEGGER, P2P-Netzwerke, 222; GLARNER, Musikpiraterie im Internet, 87 f.

<sup>255</sup> Vgl. HILGERT/GRETH, 82.

<sup>256</sup> REINBACHER, NStZ 2014, 60.

<sup>257</sup> S.o. Rz. 85.

### 3. Strafbarkeit der Betreiber von *Linksammlungen*

- 92 Über die Webseite von *kino.to* wurden bis zum 8. Juni 2011 insgesamt mindestens 1'360'450 *Links* öffentlich zugänglich gemacht.<sup>258</sup> Jeder einzelne *Link* verwies auf eine bestimmte Audio-/Videodatei, die auf einem von *kino.to* zumindest teilweise unabhängigen *Server* (sog. *Share-* oder *Filehoster*) abgespeichert worden war.

#### A. Alleintäterschaft

- 93 Gegen eine Alleintäterschaft der Betreiber der *Linksammlung* (vorliegend die Mitarbeiter von *kino.to*) lässt sich einwenden, dass diese die geschützten Werke nicht selbst auf die *Server* der *Filehoster* hochluden.<sup>259</sup> Das Einstellen bzw. Veröffentlichen von *Links* in einer *Linksammlung* stellt zudem auch keine unerlaubte Vervielfältigung i.S.v. Art. 67 Abs. 1 lit. e URG dar, da der *Link* lediglich die Verknüpfung zur abgespeicherten Datei herstellt, ohne dass es dabei zu einer Vervielfältigung einzelner Werkdaten kommt.<sup>260</sup>
- 94 Für die Annahme einer unerlaubten Zugänglichmachung i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG durch die Betreiber der *Linksammlung* spricht, dass die Nutzer ohne den fraglichen *Link* kaum je zur Darstellung des unerlaubt zugänglich gemachten Werks hätten gelangen können.<sup>261</sup> Vorliegend wurde das Werk überhaupt erst mit der Veröffentlichung des *Links* auf der Webseite von *kino.to* für die Öffentlichkeit zugänglich. Zuvor konnte dieses bloss von den *Uploadern* und den Mitarbeitern von *kino.to* abgerufen werden. Diese Tatsache rechtfertigt m.E. eine abweichende Behandlung gegenüber *Links* oder

---

<sup>258</sup> REINBACHER, NStZ 2014, 58; Urteil des LG Leipzig vom 14. Juni 2012 – KLS 390 Js 191/11, ZUM 2013, 340.

<sup>259</sup> SCHWARZENEGGER, P2P-Netzwerke, 239; GLARNER, Musikpiraterie im Internet, 143; vgl. zum deutschen Recht: REINBACHER, NStZ 2014, 59, wonach die *Verlinkung* keine Täterschaft zu begründen vermag, da für die Tathandlung des Zugänglichmachens der technische Vorgang des *Uploads* entscheidend sei.

<sup>260</sup> REINBACHER, NStZ 2014, 59, m.w.H.

<sup>261</sup> Siehe HENDEL, ZUM 2014, 104 f., nach dessen Ansicht eine *Verlinkung* dann als Zugänglichmachung qualifiziert werden muss, „wenn die Öffentlichkeit auf anderem Wege überhaupt nicht oder nur mit erheblichem Mehraufwand – also insbesondere nicht über die üblichen Suchmaschinen – zur Darstellung des geschützten Werkes gelangen kann“; siehe ferner ULLRICH, ZUM 2010, 857 f.

*Frames* mit denen lediglich ein Angebot verknüpft wird, welches bereits öffentlich zugänglich ist.<sup>262</sup>

## B. Mittelbare Täterschaft

Sind die Voraussetzungen der Alleintäterschaft nicht erfüllt, ist eine mittelbare Täterschaft zu prüfen. Die mittelbare Täterschaft ist im StGB nicht geregelt. Nach bundesgerichtlicher Rechtsprechung ist mittelbarer Täter, wer einen anderen Menschen als sein willenloses oder wenigstens nicht vorsätzlich handelndes Werkzeug benutzt, um durch ihn die beabsichtigte strafbare Handlung ausführen zu lassen.<sup>263</sup> Da von den Betreibern der *Linklisten* kein unmittelbarer Druck oder Zwang auf die *Uploader* ausgeübt worden war, ist eine mittelbare Täterschaft in der vorliegenden Konstellation ausgeschlossen. Die *Uploader* handeln vielmehr vorsätzlich aus eigenen (finanziellen) Motiven mit den Anbietern der *Linksammlung* zusammen und verfügen über die Tatherrschaft. Auch ist ihnen die Rechtswidrigkeit ihres Handelns bewusst.

## C. Mittäterschaft

Im StGB findet sich keine explizite Regelung der Mittäterschaft.<sup>264</sup> Nach bundesgerichtlicher Rechtsprechung ist Mittäter, wer die sogenannte „Tatherrschaft“ ausübt, d.h. wer bei der Entschliessung, Planung oder Ausführung eines Delikts vorsätzlich und in massgebender Weise mit anderen Tätern zusammenwirkt, sodass er als Hauptbeteiligter dasteht, wobei konkludentes Handeln genügt.<sup>265</sup>

### a) Objektiver Tatbestand

Gegen die Annahme einer Mittäterschaft kann vorliegend eingewendet werden, dass es fraglich ist, ob die Betreiber der *Linklisten* die Tat als eigene wollten oder ob sie bloss die von Dritten (*Uploadern*) begangenen Urheber-

---

<sup>262</sup> In diesen Konstellationen wirken die *Links* bzw. *Frames* lediglich „wie ein Verstärker“ auf ein bereits öffentlich zugängliches Angebot; Vgl. SCHWARZENEGGER, P2P-Netzwerke, 245 f.

<sup>263</sup> Urteil 6B.904/2010 des Bundesgerichts vom 16. Juni 2011, Erw. 3.4; BGE 120 IV 17, Erw. 2d.

<sup>264</sup> DONATSCH/TAG, 173.

<sup>265</sup> BGE 130 IV 58, Erw. 9.2.1; 133 IV 76, Erw. 2.7; 126 IV 84, Erw. 2c/aa; 125 IV 134, Erw. 3a.

rechtsverletzungen für eigene Zwecke ausnutzten.<sup>266</sup> Fraglich ist zudem, ob die Betreiber der *Linklisten* im Tatzeitpunkt über die geforderte Tatherrschaft verfügten. Die *Uploader* luden die geschützten Werke in eigener Verantwortung hoch und erhielten von den Mitarbeitern von *kino.to* keine konkreten Vorgaben bezüglich der Inhalte.<sup>267</sup> Auch konnten die hochgeladenen Dateien von den *Uploadern* und den beteiligten *Filehostern* jederzeit entfernt werden.<sup>268</sup>

- 98 Für eine Mittäterschaft spricht der Umstand, dass die *Uploader* von den Mitarbeitern von *kino.to* persönlich ausgewählt wurden. Zwischen den *Uploadern* und den Mitarbeitern von *kino.to* bestand Konsens darüber, urheberrechtlich geschützte Inhalte – durch das Aufschalten der dazugehörigen *Links* auf der Webseite von *kino.to* – einer unbeschränkten Vielzahl von Personen zugänglich zu machen. In der Phase der Planung und Organisation der Haupttat kommt den Mitarbeitern von *kino.to* ein wesentlicher Einfluss zu. Die Mitarbeiter von *kino.to* kontrollierten die übermittelten *Links* und waren für den Betrieb und den Unterhalt der Webseite verantwortlich. Durch die Veröffentlichung der *Links* auf der Webseite von *kino.to* wurden die Nutzer überhaupt erst in die Lage versetzt, die Werke aufzufinden und abzurufen. Die *Uploader*, die Mitarbeiter von *kino.to* und die *Filehoster* handelten nach einem gemeinsamen Tatplan mit dem Ziel, durch die massenhafte Verletzung von Urheberrechten im Internet Profite zu erzielen.<sup>269</sup>
- 99 Zustimmend mit dem Urteil des Amtsgerichts Leipzig vom 21. Dezember 2011 ist das gemeinsame Vorgehen der *Uploader*, der Mitarbeiter von *kino.to* und der *Filehoster* als arbeitsteiligen Vorgang zu qualifizieren und eine Mittäterschaft zu bejahen.<sup>270</sup> Dies hat zur Konsequenz, dass sich die Mitarbeiter von *kino.to* sämtliche Handlungen der *Uploader* und *Filehoster* als eigene anrechnen lassen müssen. Die unerlaubte Herstellung von Werkexemplaren gem. Art. 67 Abs. 1 lit. e URG durch das Hochladen geschützter Werke auf

---

<sup>266</sup> REINBACHER, NStZ 2014, 60.

<sup>267</sup> REINBACHER, NStZ 2014, 60.

<sup>268</sup> REINBACHER, NStZ 2014, 60; dadurch hätte der Link ins Leere geführt und wäre nutzlos geworden.

<sup>269</sup> Zum Ganzen REINBACHER, NStZ 2014, 60; Auf der Webseite von *kino.to* sowie den daran beteiligten *Servern* wurde so ein hoher Datenverkehr (traffic) mit vielen Besuchern erzielt. Durch das Aufschalten von Werbeanzeigen und den Verkauf von Premium-Abonnements wurden Einnahmen generiert und unter den beteiligten Personen aufgeteilt.

<sup>270</sup> Vgl. Urteil des AG Leipzig vom 21. Dezember 2011, 200 Ls 390 Js 184-11.

die *Server* der *Filehoster* und das unerlaubte Zugänglichmachen derselben i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG ist deshalb auch den Mitarbeitern von *kino.to* objektiv zurechenbar. Umgekehrt müssen sich die *Uploader* und *Filehoster* die Handlungen der Mitarbeiter von *kino.to* anrechnen lassen.<sup>271</sup>

**b) Subjektiver Tatbestand**

Der subjektive Tatbestand setzt einen gemeinsam getragenen Tatentschluss voraus, der auch bloss konkludent zum Ausdruck kommen kann, wobei Eventualvorsatz genügt.<sup>272</sup> Indem die Mitarbeiter von *kino.to* um die Auswahl der *Uploader* besorgt waren und die übermittelten *Links* überprüft und auf der Webseite von *kino.to* aufgeschaltet haben, manifestiert sich deren Wille, gemeinsam mit den *Uploadern* Urheberrechtsverletzungen i.S.v. Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG zu begehen. Die Betreiber der *Link*-sammlung handelten bezüglich sämtlicher objektiver Tatbestandsmerkmale mit Wissen und Wollen.<sup>273</sup>

**c) Rechtswidrigkeit und Schuld**

Es sind vorliegend kaum gesetzliche oder übergesetzliche Rechtfertigungsgründe denkbar. Ein rechtlich beachtlicher Irrtum gem. Art. 21 StGB kommt kaum je in Betracht.

**d) Gewerbsmässiges Handeln**

Aufgrund der Zeit und der Mittel, welche die Mitarbeiter von *kino.to* für das unrechtmässige Zugänglichmachen der geschützten Werke aufgewendet haben (Überprüfung der hochgeladenen *Links*, Unterhalt der Webseite, Aufschalten von Werbeanzeigen etc.) sowie des Umfangs der begangenen Urheberrechtsverletzungen (mehr als 135'000 Kinofilme und TV-Serien wurden zugänglich gemacht) und den dadurch erzielten Einnahmen (über 3,7 Mio. Euro) ist von einer gewerbsmässigen Begehung nach Art. 67 Abs. 2 URG auszugehen.<sup>274</sup>

---

<sup>271</sup> REINBACHER, NStZ 2014, 60.

<sup>272</sup> DONATSCH/TAG, 173 ff.; Urteil 6B\_735/2011 des Bundesgerichts vom 3. April 2012, Erw. 3.4.2.; Urteil 6B\_911/2009 des Bundesgerichts vom 16. Juni 2011, Erw. 2.4.

<sup>273</sup> SCHWARZENEGGER, P2P-Netzwerke, 242; GLARNER, Musikpiraterie im Internet, 87.

<sup>274</sup> REINBACHER, NStZ 2014, 57.

## D. Anstiftung

- 103 Wird mit Blick auf den Tatbeitrag der Anbieter der *Linksammlung* eine Mitäterschaft verneint, ist weiter eine Anstiftung zur Begehung von Urheberrechtsverletzungen zu prüfen. Gemäss Art. 24 Abs. 1 StGB ist Anstifter, wer jemanden vorsätzlich zu dem von diesem verübten Delikt (Verbrechen oder Vergehen) bestimmt hat.<sup>275</sup> Die Anstiftung setzt voraus, dass der Anstifter auf den nachmaligen Täter einwirkt und sich dieser im Anschluss zur Tat entschliesst und diese auch tatsächlich begeht.<sup>276</sup> Dabei ist es nicht erforderlich, dass der Anstifter zur Bewirkung des Tatentschlusses einen erheblichen Widerstand überwinden muss.<sup>277</sup> Erforderlich ist eine psychische oder kommunikative Einwirkung auf den Täter.<sup>278</sup> Nicht ausreichend für eine Anstiftung ist, wenn lediglich eine Situation geschaffen wird, in der sich der Haupttäter voraussichtlich zur Begehung einer Straftat entschliessen wird.<sup>279</sup>

### a) Objektiver Tatbestand

- 104 Vorliegend könnte die Anstiftung darin gesehen werden, dass die Mitarbeiter von *kino.to* den *Uploadern* für ihre Dienste finanzielle Entschädigungen in Aussicht gestellt haben.<sup>280</sup> Ob diese Entschädigungen von den Mitarbeitern von *kino.to* selbst oder den *Filehostern* geleistet wurden, ist irrelevant, da beide nach einem gemeinsamen Tatplan gehandelt haben und Konsens hinsichtlich der einzelnen Tatbeiträge und Vergütungen bestand.
- 105 Durch das an persönlich ausgewählte Personen abgegebene Versprechen finanzieller Vorteile für das Hochladen von urheberrechtlich geschützten Werken auf die *Server* ausgewählter *Filehoster* zum Zwecke der unerlaubten Zugänglichmachung haben die Mitarbeiter von *kino.to* auf die Willensbildung der *Uploader* eingewirkt und bei diesen den Tatentschluss zur Begehung von Urheberrechtsverletzungen i.S.v. Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG hervorgerufen.

---

<sup>275</sup> STRATENWERTH, § 13 Rz. 95; DONATSCH/TAG, 153.

<sup>276</sup> BGE 124 IV 34, Erw. 2 c.

<sup>277</sup> BGE 124 IV 34, Erw. 2 c.; 116 IV 1, Erw. 3c-d.

<sup>278</sup> STRATENWERTH, § 13 N 101.

<sup>279</sup> BGE 128 IV 11, Erw. 2a; 127 IV 122, Erw. 2b; FORSTER, BSK StGB I, Art. 24 N 15; STRATENWERTH, § 13 N 101; GLARNER, Musikpiraterie im Internet, 142.

<sup>280</sup> REINBACHER, NStZ 2014, 58.



**b) Subjektiver Tatbestand**

Die Anstiftung setzt in subjektiver Hinsicht das vorsätzliche Bestimmen eines anderen zur Begehung einer vorsätzlichen rechtswidrigen Tat voraus.<sup>281</sup> Der Vorsatz muss sich dabei auf die Herbeiführung des Tatenschlusses sowie auf die Ausführung der Tat durch den Angestifteten beziehen (Doppelvorsatz), wobei Eventualvorsatz genügt.<sup>282</sup> Da die *Uploader* persönlich von den Mitarbeitern von *kino.to* ausgewählt und instruiert wurden, ist der Vorsatz bezüglich des Bestimmens des Haupttäters erfüllt. Weiter ist auch der Vorsatz bezüglich Verübung der Haupttat gegeben, da die *Uploader* gemäss den Vorgaben der Mitarbeiter von *kino.to* handelten.<sup>283</sup>

**c) Rechtswidrigkeit und Schuld**

Es sind in dieser Konstellation kaum Rechtfertigungs- oder Schuldausschlussgründe ersichtlich. Auch ein Irrtum über die Rechtswidrigkeit ist hier ausgeschlossen.

**E. Gehilfenschaft zur unerlaubten Herstellung von Werkexemplaren auf den Servern der Filehoster**

In objektiver Hinsicht setzt die Gehilfenschaft zur unerlaubten Herstellung eines Werkexemplars gem. Art. 67 Abs. 1 lit. e URG i.V.m. Art. 25 StGB eine tatbestandsmässige rechtswidrige Haupttat und eine die Haupttat fördernde Gehilfenleistung voraus.<sup>284</sup> Nach bundesgerichtlicher Rechtsprechung gilt als Hilfeleistung jeder kausale Tatbeitrag, der die Tat fördert, sodass sich diese ohne die Mitwirkung des Gehilfen anders abgespielt hätte.<sup>285</sup> In Abgrenzung zur Mittäterschaft verlangt die Gehilfenschaft lediglich einen untergeordneten Tatbeitrag, der die Haupttat unterstützt.<sup>286</sup> Die Strafe des Gehilfen entspricht jener für die Haupttat, wobei jedoch eine Strafmilderung

---

<sup>281</sup> BGE 128 IV 11, Erw. 2a; 127 IV 122, Erw. 1; 116 IV 1, Erw. 3c-d.

<sup>282</sup> Urteil 6S.18/2005 des Bundesgerichts vom 8. Juni 2005, Erw. 4.3.2.

<sup>283</sup> Nicht entscheidend ist dabei, dass die Mitarbeiter von *kino.to* keine konkreten Vorgaben machten, welche geschützten Werke genau hochgeladen werden sollen. Die Konkretisierung, dass es sich dabei um urheberrechtlich geschützte Werke handeln soll, ist bereits ausreichend.

<sup>284</sup> SCHWARZENEGGER, P2P-Netzwerke, 240 ff.

<sup>285</sup> BGE 129 IV 124, Erw. 3.2; 121 IV 109, Erw. 3a; 120 IV 265, Erw. 2c/aa.

<sup>286</sup> STRATENWERTH, § 13 N 118.

nach Art. 48a StGB zur Anwendung kommt.<sup>287</sup> Die Beihilfe kann vor bzw. während der Ausführung der Haupttat bis zu deren Vollendung geleistet werden.<sup>288</sup>

- 109 Der Tatbestand der unerlaubten Herstellung eines Werkexemplars i.S.v. Art. 67 Abs. 1 lit. e URG ist mit dem *Upload* des Werks auf den *Server* des *Filehosters* vollendet. Da der Tatbeitrag der Betreiber der *Linklisten*, namentlich das Veröffentlichen der *Links* auf der Webseite von *kino.to*, erst zu einem Zeitpunkt stattfindet, in dem die unerlaubte Herstellung eines Werkexemplars bereits erfolgt ist, fällt eine die Haupttat fördernde physische Gehilfenschaft ausser Betracht.
- 110 Gegebenenfalls könnte eine psychische Gehilfenschaft bejaht werden, falls die Betreiber der *Linklisten* die *Uploader* – etwa durch die Zusicherung finanzieller Entschädigungen für den *Upload* geschützter Werke – in deren bereits vorhandenen deliktischen Willen bestärken.<sup>289</sup>

## **F. Gehilfenschaft zur unerlaubten Zugänglichmachung von Werken**

### **a) Objektiver Tatbestand**

- 111 Die objektiven Tatbestandsvoraussetzungen für die Gehilfenschaft zur unerlaubten Zugänglichmachung von Werken i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG i.V.m. Art. 25 StGB sind deckungsgleich mit denjenigen zur Gehilfenschaft zur unrechtmässigen Herstellung eines Werkexemplars.<sup>290</sup>
- 112 Im Unterschied zur unerlaubten Herstellung von Werkexemplaren stellt die unerlaubte Zugänglichmachung von Werken ein Dauerdelikt dar.<sup>291</sup> Bei Dauerdelikten ist die Gehilfenschaft bis zur Beendigung des Delikts möglich (i.c. das Entfernen der *Links* zu den unerlaubt zugänglich gemachten Werken von der Webseite von *kino.to*). Der Förderungsbeitrag der Mitarbeiter von *kino.to*

---

<sup>287</sup> DONATSCH/TAG, 164.

<sup>288</sup> DONATSCH/TAG, 168.

<sup>289</sup> Urteil 6P.40/2005 des Bundesgerichts vom 1. September 2005, Erw. 2.1.

<sup>290</sup> S.o. Rz. 108.

<sup>291</sup> SCHWARZENEGGER, P2P-Netzwerke, 246; eher bejahend REHBINDER/VIGANÒ, Art. 67 N 14, die für die Annahme eines Dauerdelikts plädieren, falls „der Störer fortgesetzt die Herrschaft über die Zugänglichkeit des Werks ausübt [...]“; mindestens, wenn er aktiv, bspw. durch Unterhalt und Wartung oder durch das Off- und wieder Online-Stellen des Servers, auf die Zugänglichkeit einwirkt“.

liegt im Aufschalten der *Links* zu den unerlaubt zugänglich gemachten Werken auf der Webseite von *kino.to*.<sup>292</sup> Nicht entscheidend ist dabei, dass der Abruf der illegal angebotenen Werke – zumindest theoretisch – auch ohne die Veröffentlichung der entsprechenden *Links* in der *Linksammlung* von *kino.to* möglich gewesen wäre. Der objektive Tatbestand der Gehilfenschaft zu einer unerlaubten Zugänglichmachung ist selbst dann erfüllt, wenn der Zugang zur *Linksammlung* von einer Registrierung abhängig gemacht wird. Personen, die sich zum Zwecke des Austausches von geschützten Werken über das Internet zusammenschliessen, begründen keine enge Verbundenheit i.S.v. Art. 19 Abs. 1 lit. a URG.<sup>293</sup>

**b) Subjektiver Tatbestand**

Damit der subjektive Tatbestand erfüllt ist, muss sich der (Eventual-)Vorsatz des Gehilfen sowohl auf die Haupttat wie auch auf die eigene Hilfeleistung beziehen.<sup>294</sup> Die Mitarbeiter von *kino.to* wissen Bescheid um die Rechtswidrigkeit der Zugänglichmachung und wollen diese durch das Aufschalten der *Links* fördern. Sie handeln mit der Absicht, die geschützten Werke einer möglichst grossen Zahl von Nutzern zugänglich zu machen, um so hohe Besucherzahlen (*traffic*) auf der eigenen Webseite sowie auf den Webseiten der *Filehoster* zu generieren und durch die Schaltung von Werbung und den Verkauf von Premium-Abonnements Einkünfte zu erzielen.

**c) Rechtswidrigkeit und Schuld**

Es sind in der vorliegenden Konstellation kaum Rechtfertigungs- oder Schuldabschlussgründe denkbar. Auch ein beachtlicher Rechtsirrtum erscheint – mangels Unvermeidbarkeit – als ausgeschlossen.

---

<sup>292</sup> SCHWARZENEGGER, P2P-Netzwerke, 245 f., der mit Blick auf das Anbieten sog. *Hash-Links* bei P2P-Netzwerken davon spricht, dass diese „wie ein Verstärker des Angebots“ wirken.

<sup>293</sup> REHBINDER/VIGANÒ, Art. 19 N 16.

<sup>294</sup> DONATSCH/TAG, 168; SCHWARZENEGGER, P2P-Netzwerke, 242.

## 4. Strafbarkeit der *Filehoster*

### A. Alleintäterschaft

- 115 *Filehoster*<sup>295</sup> bieten den Nutzern die Möglichkeit, Dateien auf ihre *Server* hochzuladen, abzuspeichern und bei Bedarf wieder abzurufen.<sup>296</sup> Der vom *Filehoster* zur Verfügung gestellte virtuelle Speicherplatz kann sowohl zum Zweck der externen Datensicherung als auch für einen *Cloud*-basierten Datenaustausch verwendet werden.<sup>297</sup> Nach erfolgtem *Upload* erhalten die Nutzer einen *Link*, mit dem die auf dem *Server* abgelegten Dateien abgerufen werden können.<sup>298</sup> Da die *Filehosting*-Dienste den Nutzern lediglich Speicherplatz zur Verfügung stellen und auf die hochgeladenen Inhalte selbst keinen Einfluss haben, ist eine Urheberrechtsverletzung nach Art. 67 URG in Alleintäterschaft i.d.R. ausgeschlossen.
- 116 Vorliegend muss bei der Bewertung der Strafbarkeit jedoch mitberücksichtigt werden, dass die *Filehoster* die *Uploader* für das Hochladen von urheberrechtlich geschützten Inhalten finanziell entschädigt hatten. In solchen Fällen ist die unerlaubte Zugänglichmachung eines Werks durch Unterlassung zu prüfen (Art. 67 Abs. 1 lit. g<sup>bis</sup> URG i.V.m. Art. 11 Abs. 2 lit. d StGB). Entscheidend ist dabei, ob die *Filehoster* rechtlich zu einem Eingreifen gegen die über ihre *Server* begangenen Urheberrechtsverletzungen verpflichtet sind. Nach Art. 11 Abs. 2 StGB kann eine Garantenstellung u.a. aufgrund des Gesetzes sowie durch die Schaffung einer Gefahr (sog. Ingerenz) entstehen. Eine gesetzliche Grundlage, welche die *Filehoster* verpflichtet, Rechtsverletzungen reaktiv zu beseitigen oder gar proaktiv zu verhindern, ist nicht ersichtlich.<sup>299</sup> Bei einer Garantenstellung aus Ingerenz muss dem *Filehoster* ein vorausgegangenes, pflichtwidriges, gefährdendes Tun zum Vorwurf gemacht werden können.<sup>300</sup> Zwar ist dem Betrieb eines

---

<sup>295</sup> Unter den Begriff *Filehoster* fallen Anbieter wie Dropbox, uploaded, Wuala, RapidShare (Service eingestellt am 31. März 2015), Rapidgator, BitShare, Mega, Swissload, DepositFiles, Netload etc.

<sup>296</sup> WULLSCHLEGER, Rz. 239; OBERGFELL, NJW 2013, 1995.

<sup>297</sup> SCHEDER-BIESCHIN, 79; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 4.

<sup>298</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 16; OBERGFELL, NJW 2013, 1995.

<sup>299</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 40, wonach „im Grundsatz keine Pflicht [besteht], handelnd einzugreifen, um einen anderen vor Schaden zu bewahren“; BGE 115 II 15, Erw 3.b.

<sup>300</sup> FOUNTOULAKIS/FRANCEY, medialex 2014, 179, m.w.H.

*Filehosting-Dienste* die Gefahr von Urheberrechtsverletzungen inhärent. Solange der *Filehoster* aber nicht pflichtwidrig handelt – etwa indem er dafür wirbt, dass über seinen Dienst urheberrechtlich geschützte Werke ausgetauscht werden können, oder indem er besondere Anreize zur Begehung von Urheberrechtsverletzungen schafft – ist eine Garantenstellung aus Ingerenz zu verneinen.<sup>301</sup> Vorliegend haben die *Filehoster* den *Uploadern* für das Hochladen und Zugänglichmachen von urheberrechtlich geschützten Werken eine finanzielle Entschädigung angeboten. Dadurch haben die *Filehoster* besondere Anreize für die Begehung von Urheberrechtsverstößen geschaffen, womit eine Garantenstellung aus Ingerenz zu bejahen ist. Falls der *Filehoster* die unerlaubt über seine *Server* zugänglich gemachten Werke nicht entfernt, ist dieser wegen einer unerlaubten Zugänglichmachung von Werken durch Unterlassung zu bestrafen.

## B. Mittäterschaft

### a) Objektiver Tatbestand

Das Bundesgericht hielt in seinem Entscheid vom 14. Januar 2013 gegen die Genfer Tageszeitung „*Tribune de Genève*“ fest, dass diese durch das Zurverfügungstellen von Speicherplatz für einen (fremden) *Blog* die öffentliche Verbreitung eines inkriminierten *Blog*-Beitrages gegenüber einem breiten Leserkreis ermöglicht habe, weshalb sie als Betreiberin des *Blogs* auch für die von Dritten verfassten Blogbeiträge zivilrechtlich mitverantwortlich sei.<sup>302</sup> 117

Mit Blick auf das Urheberstrafrecht ist eine verschuldensunabhängige Haftung sämtlicher Personen, die bei einer Urheberrechtsverletzung mitgewirkt haben – etwa wenn die Mitwirkung bloss untergeordneter Natur ist und sich beispielsweise auf das Zurverfügungstellen der technischen Infrastruktur beschränkt – abzulehnen. Da es sich bei den Urheberrechtsdelikten ausnahmslos um Vorsatzdelikte handelt, wird eine vorgängige Kenntnisnahme der Urheberrechtsverletzung vorausgesetzt. Durch die bloss abstrakte Gefahr, dass die *Server* der *Filehoster* für Urheberrechtsverstösse verwendet 118

---

<sup>301</sup> WULLSCHLEGER, Rz. 241, sieht die Grenze zwischen erlaubter und unerlaubter Anreizsetzung dann überschritten, „wenn aus einem Angebot unmissverständlich hervorgeht, dass das Heraufladen von urheberrechtlich geschützten Werken honoriert wird“.

<sup>302</sup> Vgl. FOUNTOLAKIS/FRANCEY, *medialex* 2014, 178 ff.; HUG, *medialex* 2014, 56 f.; KERNEN, *Jusletter* vom 4. März 2013, Rz. 9; Urteil 5A\_792/2011 des Bundesgerichts vom 14. Januar 2013, Erw. 6.3.

werden, nehmen die Betreiber noch keine Urheberrechtsverletzungen in Kauf.

- 119 Vorliegend sprechen aber zahlreiche Indizien dafür, das Zusammenwirken der *Uploader*, der Anbieter der *Linklisten* und der *Filehoster* als arbeitsteiligen Vorgang zu qualifizieren.<sup>303</sup> Die Beteiligten handelten nach einem gemeinsamen Tatplan, bei dem jeder innerhalb des Unternehmens eine ihm zugewiesene Rolle einnahm. Der objektive Tatbeitrag der *Filehoster* bestand darin, dass diese die hochgeladenen Werke konvertiert und auf ihren *Servern* für eine unbestimmte Anzahl von Nutzern zum Abruf bereitgehalten haben.<sup>304</sup> Das Konzept der Mittäterschaft bewirkt, dass sich der Mittäter nicht durch den Einwand befreien kann, ein anderer habe die fragliche Tathandlung ausgeführt, weshalb er hierfür nicht zur Rechenschaft gezogen werden könne.<sup>305</sup>

#### **b) Subjektiver Tatbestand**

- 120 In subjektiver Hinsicht setzt der Tatbestand von Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG ein vorsätzliches Handeln voraus, wobei Eventualvorsatz genügt.<sup>306</sup> Die *Filehoster* wussten, dass die geschützten Werke ohne die Einwilligung der Rechteinhaber hochgeladen und einer unbestimmten Vielzahl von Personen zugänglich gemacht werden sollten. Sie handelten vorsätzlich mit den *Uploadern* und den Betreibern der *Linksammlung* zusammen, um gemeinsam Urheberrechtsverletzungen zu begehen.

#### **c) Rechtswidrigkeit und Schuld**

- 121 Es sind vorliegend kaum Rechtfertigungs- oder Schuldausschlussgründe denkbar. Ein Irrtum über die Rechtswidrigkeit nach Art. 21 StGB scheint ebenso ausgeschlossen.

#### **d) Gewerbsmässiges Handeln**

- 122 Die gewerbsmässige Begehung von Urheberrechtsverletzungen i.S.v. Art. 67 Abs. 2 URG ist vorliegend auch mit Blick auf die *Filehoster* zu bejahen.

---

<sup>303</sup> S.o. Rz. 98 f.

<sup>304</sup> REINBACHER, NStZ 2014, 62.

<sup>305</sup> Urteil 6B.939/2013 des Bundesgerichts vom 17. Juni 2014, Erw. 2.

<sup>306</sup> SCHWARZENEGGER, P2P-Netzwerke, 222; GLARNER, Musikpiraterie im Internet, 87 f.

Diese erzielten beträchtliche Einnahmen durch das Aufschalten von Werbeanzeigen sowie den Verkauf von Premium-Mitgliedschaften.<sup>307</sup>

### C. Anstiftung

Falls eine Mittäterschaft verneint wird, ist eine Anstiftung zu prüfen. Durch das Versprechen oder Gewähren von Vorteilen für das Hochladen von urheberrechtlich geschützten Werken haben die *Filehoster* auf die Willensbildung der *Uploader* eingewirkt und bei diesen den Tatentschluss zur Begehung von Urheberrechtsverletzungen i.S.v. Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG hervorgerufen. Dabei ist irrelevant ob die Auswahl der *Uploader* durch die *Filehoster* selbst oder durch die Mitarbeiter von *kino.to* vorgenommen wurden da beide nach einem gemeinsamen Tatplan handelten.<sup>308</sup>

### D. Gehilfenschaft zur unerlaubten Herstellung von Werkexemplaren

#### a) Objektiver Tatbestand

Die Gehilfenschaft setzt in objektiver Hinsicht eine tatbestandsmässige rechtswidrige Haupttat sowie eine die Haupttat fördernde Leistung des Gehilfen voraus.<sup>309</sup> Als physische Gehilfenschaft kommt jede äusserliche Förderung der Tat in Betracht.<sup>310</sup> Der Förderungsbeitrag der *Filehoster* liegt in der Zurverfügungstellung von virtuellem Speicherplatz zum Zwecke der unerlaubten Herstellung von Werkexemplaren.

Alternativ kann das Versprechen bzw. das Ausrichten finanzieller Vorteile an die *Uploader* auch als psychische Gehilfenschaft gewertet werden. Dadurch bestärkten die *Filehoster* die *Uploader* in ihrem bereits vorhandenen deliktischen Willen, unerlaubt urheberrechtlich geschützte Werke über das Internet zugänglich zu machen.

#### b) Subjektiver Tatbestand

In subjektiver Hinsicht ist erforderlich, „dass der Gehilfe weiss oder damit rechnet, eine bestimmt geartete Straftat zu unterstützen, und dass er dies will

---

<sup>307</sup> S.o. Rz. 80.

<sup>308</sup> S.o. Rz. 103 ff.

<sup>309</sup> SCHWARZENEGGER, P2P-Netzwerke, 240; ders., E-Commerce, 354.

<sup>310</sup> BGE 104 IV 156, Erw. 3; 108 Ib 301, Erw. 3.

oder in Kauf nimmt, wobei zum Vorsatz auch die Voraussicht des Geschehensablaufs gehört [...]“<sup>311</sup>.

- 127 Die *Filehoster* haben Kenntnis davon, dass die auf ihren *Servern* hergestellten Werkkopien zum Zwecke der unerlaubten Zugänglichmachung über das Internet verwendet werden. Die *Filehoster* handeln vorsätzlich hinsichtlich des Handelns der Haupttäter (*Uploader*) und der Hilfeleistung.

### c) *Rechtswidrigkeit und Schuld*

- 128 Es sind weder Rechtfertigungs- noch Schuldausschlussgründe ersichtlich. Ein rechtlich beachtlicher Irrtum ist kaum denkbar.

## E. **Gehilfenschaft zur unerlaubten Zugänglichmachung von Werken**

### a) *Objektiver Tatbestand*

- 129 Der objektive Tatbestand der Gehilfenschaft setzt eine Förderung der Tat handlung durch physische oder psychische Unterstützung voraus.<sup>312</sup> Die physische Gehilfenschaft der *Filehoster* kann darin gesehen werden, dass diese die hochgeladenen Filme in ein für das Streaming geeignetes Dateiformat konvertiert und anschliessend auf ihren *Servern* zum Abruf über das Internet bereitgehalten haben.<sup>313</sup>
- 130 Die gesteigerte Wahrscheinlichkeit, dass die unerlaubt zugänglich gemachten Werke von Dritten abgerufen werden genügt, um eine objektive Unterstützung der Handlungen der Haupttäter zu bejahen.<sup>314</sup> Die Hilfeleistung der *Filehoster* liegt im aktiven Bereithalten der unerlaubt über ihre Server zugänglich gemachten Werke zum Abruf durch beliebige Dritte. Da Art. 67 Abs. 1 lit. g<sup>bis</sup> URG als Dauerdelikt ausgestaltet ist, können die *Filehoster* solange Beihilfe leisten, bis die unerlaubt zugänglich gemachten Werke auf den *Servern* gelöscht werden.

---

<sup>311</sup> Urteil 6P.40/2005 des Bundesgerichts vom 1. September 2005, Erw. 2.1.

<sup>312</sup> Urteil 6P.40/2005 des Bundesgerichts vom 1. September 2005, Erw. 2.1.

<sup>313</sup> REINBACHER, NStZ 2014, 57.

<sup>314</sup> SCHWARZENEGGER, P2P-Netzwerke, 246; FLECHSIG/GABEL, CR 1998, 356.



**b) Subjektiver Tatbestand**

Die *Filehoster* wollen die über ihre *Server* begangenen Urheberrechtsverletzungen unterstützen bzw. nehmen dies zumindest in Kauf. Sie handeln mit Wissen und Wollen betreffend die unerlaubte Zugänglichmachung i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG durch die *Uploader* als Haupttäter sowie hinsichtlich ihrer eigenen Hilfeleistung. 131

**c) Rechtswidrigkeit und Schuld**

Sowohl Rechtfertigungs- oder Schuldausschlussgründe als auch ein rechtlich beachtlicher Irrtum i.S.v. Art. 21 StGB sind in dieser Fallkonstellation kaum je denkbar. 132

**5. Strafbarkeit der Werbekunden auf illegalen Streaming-Diensten**

Die Betreiber der Webseite von *kino.to* und die *Filehoster* erzielten beträchtliche Einnahmen durch den Verkauf von Werbeanzeigen.<sup>315</sup> Die Werbekunden bilden einen wichtigen Bestandteil innerhalb des Geschäftsmodells der illegalen Streaming-Anbieter, weshalb deren urheberstrafrechtliche Verantwortlichkeit näher beleuchtet werden soll. 133

**A. Alleintäterschaft oder Mittäterschaft**

Eine Alleintäterschaft ist ausgeschlossen, da die Werbekunden selbst keine urheberrechtlich geschützten Werke vervielfältigten oder öffentlich zugänglich machen. Auch eine Mittäterschaft ist mit Blick auf die Werbekunden zu verneinen, da diese zu keinem Zeitpunkt über die Tatherrschaft verfügen und ihnen in den einzelnen Tatphasen kein wesentlicher Einfluss über das Tatgeschehen zukommt. 134

**B. Gehilfenschaft zur unerlaubten Herstellung und Zugänglichmachung von Werken**

Der Tatbeitrag der Werbekunden könnte aber den Tatbestand der Gehilfenschaft zu einer unerlaubten Herstellung bzw. einer Zugänglichmachung von 135

---

<sup>315</sup> REINBACHER, NStZ 2014, 57, führt aus, dass es sich bei der Werbung überwiegend um pornografische Webseiten und „Abzockerangebote“ handelt.

Werken i.S.v. Art. 67 Abs. 1 lit. e bzw. lit. g<sup>bis</sup> URG i.V.m. Art. 25 StGB erfüllen.

#### **a) Objektiver Tatbestand**

- <sup>136</sup> Gemäss Art. 25 StGB ist als Gehilfe strafbar, wer zu einem Verbrechen oder Vergehen vorsätzlich Hilfe leistet. Die Hilfeleistung muss die Erfolgchancen der tatbestandserfüllenden Handlung erhöhen.<sup>316</sup> Der fördernde Tatbeitrag der Werbekunden beschränkt sich vorliegend auf die finanzielle Unterstützung der Betreiber der *Linksammlung* und der *Filehoster*. Zwar wird die unerlaubte Herstellung von Werkexemplaren und das unerlaubte Zugänglichmachen geschützter Werke über das Internet nicht unmittelbar gefördert. Dennoch fördern die Werbekunden diese Tathandlungen zumindest mittelbar, indem sie die Unternehmung von *kino.to* durch ihre finanzielle Beteiligung „am Laufen halten“.<sup>317</sup>
- <sup>137</sup> Für die Bewertung des Tatbeitrags der Werbekunden muss – ausgehend von den konkreten Gegebenheiten des Einzelfalls – eine gesamtheitliche Betrachtung aller Vorgänge vorgenommen werden. Entscheidend ist dabei, dass die Unternehmung von *kino.to* auf die massenhafte Verletzung von Urheberrechten ausgerichtet war, indem geschützte Werke unerlaubt und über einen längeren Zeitraum hinweg einer Vielzahl von Nutzern zugänglich gemacht wurden. Ohne die Mitwirkung der Werbekunden hätte diese Unternehmung nicht in dem Umfang betrieben werden können. Die an *kino.to* und die *Filehoster* geleisteten Zahlungen der Werbekunden sind deshalb als kausale Hilfeleistung zur massenhaften Begehung von Urheberrechtsverletzungen nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG zu qualifizieren.

#### **b) Subjektiver Tatbestand**

- <sup>138</sup> In subjektiver Hinsicht muss sich der Vorsatz des Gehilfen sowohl auf die Haupttat wie auch auf die eigene Beihilfehandlung beziehen, wobei Eventualvorsatz genügt.<sup>318</sup> Die Werbekunden haben bei der Buchung der Werbeanzeigen auf der Webseite von *kino.to* zumindest in Kauf genommen, dass über diese Webseite urheberrechtlich geschützte Werke ohne Einwilligung der

---

<sup>316</sup> BGE 129 IV 124, Erw. 3.2; 120 IV 265, Erw. 2c/aa.

<sup>317</sup> Die finanziellen Mittel der Werbekunden werden benötigt, um die Kosten für die *Servermieten*, die Vergütungen an die *Uploader* und die Personalkosten der Betreiber der *Linksammlungen* etc. zu bezahlen.

<sup>318</sup> SCHWARZENEGGER, P2P-Netzwerke, 242.

Rechteinhaber zugänglich gemacht werden. In Bezug auf die eigene Hilfeleistung haben die Werbekunden zumindest in Kauf genommen, dass durch ihre Zahlungen der Betrieb der illegalen Plattform gefördert wird.

**c) *Rechtswidrigkeit und Schuld***

Vorliegend sind kaum Rechtfertigungs- oder Schuldtausschlussgründe denkbar. Auch ein rechtlich beachtlicher Irrtum i.S.v. Art. 21 StGB scheint ausgeschlossen, da die Werbekunden zumindest laienhaft hätten erkennen können, dass die auf *kino.to* verlinkten Angebote ohne Einwilligung der Rechteinhaber zugänglich gemacht worden sind und der Betrieb der illegalen Plattform durch ihre Zahlungen unterstützt wird. 139

**6. Beteiligung an einer kriminellen Organisation**

Durch Art. 260<sup>ter</sup> Ziff. 1 StGB werden Verhaltensweisen mit Strafe bedroht, die sich im Vorfeld einer konkreten Straftat abspielen.<sup>319</sup> Der objektive Straftatbestand setzt nach Abs. 1 von letztgenannter Bestimmung die Beteiligung an einer kriminellen Organisation voraus, die ihren Aufbau und ihre personelle Situation geheim hält und deren Hauptzweck darin besteht, Gewaltverbrechen zu begehen oder sich mit verbrecherischen Mitteln zu bereichern.<sup>320</sup> Eine Beteiligung an einer kriminellen Organisation liegt vor, wenn eine Person „funktionell in die kriminelle Organisation eingegliedert [ist] und im Hinblick auf deren verbrecherische Zwecke Aktivitäten [entfaltet]“<sup>321</sup>. Nach Art. 260<sup>ter</sup> Ziff. 1 Abs. 2 StGB wird bestraft, wer eine solche Organisation in ihrer verbrecherischen Tätigkeit unterstützt.<sup>322</sup> 140

---

<sup>319</sup> ENGLER, BSK StGB II, Art. 260<sup>ter</sup> N 4, wonach ein Verhalten bestraft wird, „bevor tatsächlich ein konkretes Delikt ausgeübt worden ist“.

<sup>320</sup> STRATENWERTH/BOMMER, § 40 N 23, nach deren Ansicht es nicht genügt, dass in einem anderen Zwecken dienenden Zusammenschluss oder Betrieb auch Delikte begangen werden; DONATSCH/WOHLERS, 205, der Zweck der Organisation muss auf die Begehung von Verbrechen i.S.v. Art. 10 Abs. 2 StGB gerichtet sein; Botschaft StGB 1993, 298.

<sup>321</sup> BGE 132 IV 132, Erw. 4.1.3; ENGLER, BSK StGB II, Art. 260<sup>ter</sup> N 12; STRATENWERTH/BOMMER, § 40 N 25, m.w.H.

<sup>322</sup> BGE 132 IV 132, Erw. 4.1.4; ENGLER, BSK StGB II, Art. 260<sup>ter</sup> N 13, plädiert dafür, dass sich die Unterstützung auf die verbrecherische Tätigkeit der Organisation beziehen muss, ohne dass „ein kausaler Tatbeitrag auf ein bestimmtes Einzeldelikt nachgewiesen werden muss; STRATENWERTH/BOMMER, § 40 N 26 und DONATSCH/WOHLERS, 207 f., die beide einen unmittelbaren Zusammenhang mit der verbrecherischen Tätigkeit der

- 141 Eine kriminelle Organisation i.S.v. Art. 260<sup>ter</sup> StGB setzt „eine strukturierte Gruppe von mindestens drei, im Allgemeinen mehr, Personen voraus, die mit dem Ziel geschaffen wurde, unabhängig von einer Änderung ihrer Zusammensetzung dauerhaft zu bestehen, und die sich namentlich durch die Unterwerfung ihrer Mitglieder unter Anweisungen, durch systematische Arbeitsteilung, durch Intransparenz und durch in allen Stadien ihrer verbrecherischen Tätigkeit vorherrschende Professionalität auszeichnet“<sup>323</sup>. Sodann gehört zum Begriff der Verbrechensorganisation „eine qualifizierte und systematische Verheimlichung, die sich nicht notwendig auf das Bestehen der Organisation selbst, wohl aber auf deren interne Struktur sowie den Kreis ihrer Mitglieder und Helfer erstrecken muss“<sup>324</sup>.
- 142 Mit der Unternehmung von *kino.to* verfolgten die Beteiligten das gemeinsame Ziel, durch die massenhafte Begehung von Urheberrechtsverletzungen Einkünfte zu erzielen, indem sie unerlaubt urheberrechtlich geschützte Werke über das Internet als *Stream* oder *Download* öffentlich zugänglich gemacht hatten (Art. 67 Abs. 1 lit. g<sup>bis</sup> i.V.m. Art. 67 Abs. 2 URG). Seit 1. Juli 2008 sieht das Urheberrechtsgesetz in Art. 67 Abs. 2 URG bei gewerbsmäßig begangenen Urheberrechtsverletzungen eine Freiheitsstrafe bis zu fünf Jahren vor, womit es sich um ein Verbrechen i.S.v. Art. 10 Abs. 2 StGB handelt.<sup>325</sup> Vorliegend einschlägig ist deshalb die Beteiligung an einer kriminellen Organisation zum Zweck der Bereicherung mit verbrecherischen Mitteln.
- 143 In concreto hatten sich die Betreiber der *Linksammlung*, die *Uploader* sowie die *Filehoster* zusammengeschlossen. Die Organisation war streng hierarchisch aufgebaut, waren es doch die Betreiber der *Linksammlung*, welche die *Uploader* persönlich auswählten und über die Zusammenarbeit mit den *Filehostern* entschieden. Ebenso lag eine strikte Rollen- bzw. Arbeitsteilung innerhalb der Organisation vor.<sup>326</sup> Die Unternehmung von *kino.to* zeichnete sich zudem dadurch aus, dass sie mit dem Ziel geschaffen wurde, unabhän-

---

Organisation fordern. Nicht erforderlich ist demgegenüber ein Zusammenhang „mit einem konkreten, von der Organisation geplanten oder durchgeführten Delikt“.

<sup>323</sup> BGE 132 IV 132, Erw. 4.1.1.; ENGLER, BSK StGB II, Art. 260<sup>ter</sup> N 6, m.w.H.; STRATENWERTH/BOMMER, § 40 N 21; TRECHSEL/VEST, PK StGB, Art. 260<sup>ter</sup> N 3 f.; DONATSCH/WOHLERS, 204 ff.; Botschaft StGB 2005, 6716; Botschaft StGB 1993, 297.

<sup>324</sup> BGE 132 IV 132, Erw. 4.1.1.; ENGLER, BSK StGB II, Art. 260<sup>ter</sup> N 8; TRECHSEL/VEST, PK StGB, Art. 260<sup>ter</sup> N 5.

<sup>325</sup> DAVID, SHK URG, Art. 67 N 35; BARRELET/EGLOFF, Art. 67 N 9, m.w.H.; REHBINDER/VIGANÒ, Art. 67 N 19.

<sup>326</sup> S.o. Rz. 98 f.

gig von einer Änderung ihrer Zusammensetzung, dauerhaft zu bestehen.<sup>327</sup> Die einzelnen *Uploader*, die Mitarbeiter von *kino.to* sowie die *Filehoster* konnten grundsätzlich jederzeit ausgetauscht werden, ohne dass das Unternehmen in seinem Bestand gefährdet wurde.<sup>328</sup> Die Betreiber der *Linksammlung* verwendeten bewusst die *Top-Level-Domain* „to“, weil sich die Behörden von Tonga bekanntermassen weigern, gegen illegale Seiten vorzugehen und die Daten der Betreiber von Internetseiten geheim halten.<sup>329</sup> Die *Uploader* luden die geschützten Werke anonym auf die *Server* der *Filehoster* hoch und diese wiederum wählten Serverstandorte in Ländern, in denen sie keine strafrechtlichen Konsequenzen zu befürchten hatten.<sup>330</sup> Folglich ist in Bezug auf *kino.to* eine qualifizierte und systematische Verheimlichung der internen Struktur sowie ihrer Mitglieder und Helfer zu bejahen. Der Personenzusammenschluss bestehend aus den Betreibern der *Linksammlung*, den *Uploadern* und den *Filehostern* zum Zwecke der Erzielung von Einkünften durch die massenhafte Begehung von Urheberrechtsverletzungen erfüllt den objektiven Tatbestand der Beteiligung an einer kriminellen Organisation i.S.v. Art. 260<sup>ter</sup> Ziff. 1 Abs. 1 StGB. Die finanzielle Unterstützung der kriminellen Organisation von *kino.to* durch die Werbekunden erfüllt sodann den objektiven Tatbestand von Art. 260<sup>ter</sup> Ziff. 1 Abs. 2 StGB.

In subjektiver Hinsicht ist bei beiden Tatbestandsvarianten – Beteiligung an einer kriminellen Organisation sowie Unterstützung einer solchen – Vorsatz i.S.v. Art. 12 Abs. 2 StGB bezüglich sämtlicher objektiver Tatbestandsmerkmale erforderlich, wobei Eventualvorsatz genügt.<sup>331</sup> Sämtliche an der Organisation von *kino.to* beteiligten Personen hatten Kenntnis von der Unrechtmässigkeit ihres Tuns, womit der subjektive Tatbestand erfüllt ist.

<sup>327</sup> BGE 132 IV 132, Erw. 5.2, in Abgrenzung zu anderen kriminellen Zusammenschlüssen führt die Auswechslung einzelner oder der Ersatz ausgeschiedener Personen bei einer kriminellen Organisation nicht dazu, dass diese sich nach einem Wechsel in der Zusammensetzung der Mitglieder wieder neu konstituieren muss.

<sup>328</sup> Bereits kurze Zeit nachdem der Gründer von *kino.to* verurteilt und die Webseite von *kino.to* vom Netz genommen wurde, gab es mit *kinox.to* bereits wieder einen Nachfolger; vgl. REINBACHER, NStZ 2014, 57; STIEPER, MMR 2012, 12.

<sup>329</sup> WANDTKE/VON GERLACH, GRUR 2013, Fn. 68; STOLZ, MMR 2013, 357; RADMANN, ZUM 2010, 388, Fn. 5.

<sup>330</sup> Zur Verschleierung der Serverstandorte werden zudem Proxy-, Bouncer- (BNC) und Cloud-Dienste verwendet. Vgl. dazu KÜHL, <<http://www.zeit.de/digital/internet/2014-10/kinox-streaming-illegal-razzia>> (besucht 25. August 2015).

<sup>331</sup> BGE 132 IV 132, Erw. 4.1.4.

- <sup>145</sup> Da weder gesetzliche noch übergesetzliche Rechtfertigungsgründe in Betracht kommen und ein Rechtsirrtum nach Art. 21 StGB ausgeschlossen ist, sind die Anbieter der *Linksammlung*, die *Uploader* sowie die *Filehoster* nach Art. 260<sup>ter</sup> Ziff. 1 Abs. 1 StGB wegen Beteiligung an einer kriminellen Organisation und die Werbekunden nach Art. 260<sup>ter</sup> Ziff. 1 Abs. 2 StGB wegen Unterstützung einer kriminellen Organisation zu bestrafen.

### III. Live-Streaming von urheberrechtlich geschützten Werken durch Private

#### 1. Übersicht

- <sup>146</sup> Streaming-Apps wie etwa *Meerkat*, *Periscope* oder *YouNow* ermöglichen den Nutzern, beliebige Inhalte live und in Echtzeit über das Internet zu verbreiten.<sup>332</sup> Neben einer Vielzahl legaler Anwendungsbereiche können diese Programme auch als Werkzeuge zur Begehung von Urheberrechtsverletzungen verwendet werden.<sup>333</sup> So lassen sich etwa sämtliche Audio-/Video-Dateien aufzeichnen und als Live-Stream öffentlich zugänglich machen.<sup>334</sup> Überdies können TV-Sendungen kostenpflichtiger Bezahlsender aufgezeichnet und mittels Live-Streaming ins Internet übertragen werden.<sup>335</sup> Neben

---

<sup>332</sup> Vgl. etwa <<http://meerkatapp.co>>, <<https://www.periscope.tv>> sowie <<http://www.younow.com/about>> (alle besucht 11. Februar 2018); die Funktionsweise ist denkbar einfach: Nach Eingabe eines kurzen Erklärungstextes über den Inhalt muss lediglich der Startknopf betätigt werden und das Smartphone überträgt das Kamerabild und den Umgebungston als Live-Stream an alle, die zuschauen wollen.

<sup>333</sup> So wurden etwa vier Folgen der beliebten TV-Serie „Game of Thrones“ des Bezahlfernsehsenders HBO über das Live-Streaming-Tool Periscope ins Internet gestreamt und so einer Vielzahl von Personen zugänglich gemacht. Vgl. dazu SHAW/KHARIF, <<http://www.bloomberg.com/news/articles/2015-04-13/twitter-s-periscope-responds-to-game-of-thrones-piracy-reports>> (besucht 25. August 2015).

<sup>334</sup> A.A. BARRELET/EGLOFF, Art. 10 N 26a, die das Vorliegen eines Sendevorganges bei Live-Streams über das Internet verneinen, weil die Übermittlung nicht virtuell an beliebige Personen erfolgen würde, die lediglich ihr Empfangsgerät einzuschalten brauchen. Dieser Vorgang sei als Wahrnehmbarmachung i.S.v. Art. 10 Abs. 2 lit. c URG zu qualifizieren, da ein „zielgerichteter und individueller Daten-Transfer“ ausschliesslich an jene Empfänger vorliegen würde, die das Angebot aktiv abrufen; REHBINDER/VIGANÒ, Art. 69a N 2.

<sup>335</sup> Nebst Spielfilmen können auch Kinovorführungen, Konzerte, Boxkämpfe und andere Veranstaltungen mittels Live-Stream öffentlich zugänglich gemacht werden; STEIER, Pe-

Urheberrechtsverletzungen kann das Live-Streaming von Videos etwa auch Persönlichkeitsverletzungen zur Folge haben.<sup>336</sup>

## 2. Rechtliche Bewertung

### A. Betroffene Verwertungsrechte

#### a) *Vervielfältigungsrecht (Art. 10 Abs. 2 lit. a URG)*

Das Vervielfältigungsrecht nach Art. 10 Abs. 2 lit. a URG umfasst Vervielfältigungen auch dann, wenn diese bloss vorübergehender Natur sind.<sup>337</sup> Die Verbreitung der Mediendateien mittels Live-Streaming an die Nutzer erfordert, dass stets einige Sekunden der übertragenen Inhalte auf den *Servern* der Betreiber zwischengespeichert werden.<sup>338</sup> Für die rechtliche Beurteilung einer Vervielfältigungshandlung sollte nicht die Grösse der einzelnen zwischengespeicherten Werkfragmente entscheidend sein, sondern der Umstand, dass „in der Gesamtbetrachtung der einzelnen Vorgänge das ganze Werk bzw. schutzfähige Teile davon vervielfältigt werden“<sup>339,340</sup> Sofern beim Live-Streaming urheberrechtlich geschützte Inhalte sukzessive auf die *Server* der Anbieter hochgeladen werden, ist das Vorliegen einer rechtlich relevanten Vervielfältigung i.S.v. Art. 10 Abs. 2 lit. a URG zu bejahen. Darüber hinaus ist bei *Periscope* – im Unterschied zu *Meerkat* – das Vorliegen einer rechtlich relevanten Vervielfältigung schon deshalb zu bejahen, weil die hochgeladenen Inhalte während 24 Stunden auf den *Periscope-Servern* gespeichert bleiben und als On-Demand-Stream abgerufen werden können.<sup>341</sup>

---

riscope, <<http://www.nzz.ch/digital/boxkampf-floyd-mayweather-jr-und-manny-pacquiao-periscope-meerkat-1.18535113>> (besucht 25. August 2015).

<sup>336</sup> Werden im öffentlichen Raum Personen gefilmt, muss deren Einverständnis eingeholt werden, sofern diese auf den Aufnahmen erkennbar sind (Art. 28 ZGB); ferner sind die Straftatbestände nach Art. 135 StGB bzw. Art. 197 StGB einschlägig, falls die *Live-Streaming-Apps* dazu verwendet werden, um Gewaltdarstellungen oder Pornografie aufzuzeichnen und als Live-Stream im Internet zu verbreiten.

<sup>337</sup> S.o. Rz. 46.

<sup>338</sup> VON APPEN/BARATH, CaS 2014, 253 f.; EICHELBERGER, 28, 30 f.; a.A. BÜSCHER/MÜLLER, GRUR 2009, 559.

<sup>339</sup> STOLZ, MMR 2013, 355.

<sup>340</sup> S.u. Rz. 163 f.

<sup>341</sup> PIERCE, <<https://www.wired.com/2015/03/periscope/>> (besucht 25. August 2015); dies hat zur Folge, dass beim Streaming von urheberrechtlich geschützten Inhalten mittels

**b) Senderecht (Art. 10 Abs. 2 lit. d URG)**

- 148 Wird ein bereits aufgezeichnetes, geschütztes Werk durch Radio, Fernsehen oder ähnliche Einrichtungen zeitgleich einer unbestimmt grossen Anzahl von Personen zugänglich gemacht und bestimmt der Anbieter, wann die Übertragung beginnt, ist das Senderecht nach Art. 10 Abs. 2 lit. d URG tangiert.<sup>342</sup> Beim Live-Streaming legt der Anbieter fest, wann die Wiedergabe beginnt. Die mittels *Meerkat*- oder *Periscope-App* gestreamten Inhalte können grundsätzlich von jedermann wahrgenommen werden, womit auch das Kriterium der Öffentlichkeit erfüllt ist.<sup>343</sup> Die aktive Beteiligung der Empfänger des Live-Streams lässt sich mit dem Konsum des klassischen Fernsehens oder Rundfunks vergleichen, da diese – analog zur Programmwahl mittels Fernbedienung – lediglich auswählen müssen, welchen Live-Stream sie sich ansehen wollen.<sup>344</sup> Folglich liegt beim Live-Streaming geschützter Werke mittels *Live-Streaming-App* ein Eingriff in das Senderecht vor.

**c) Weitersenderecht (Art. 10 Abs. 2 lit. e URG)**

- 149 Dem Urheber steht gemäss Art. 10 Abs. 2 lit. e URG das ausschliessliche Recht zu, gesendete Werke mit Hilfe von technischen Einrichtungen weiterzusenden. Die Weitersendung von in- oder ausländischen Sendesignalen hat dabei durch einen anderen als den ursprünglichen Sender zu erfolgen.<sup>345</sup> Gemäss Art. 22 Abs. 1 URG können die Rechte, gesendete Werke zeitgleich und unverändert wahrnehmbar zu machen, nur von zugelassenen Verwer-

---

*Periscope-App* auch das Recht der Zugänglichmachung nach Art. 10 Abs. 2 lit. c URG tangiert ist. Wird ein gespeicherter Stream zeitversetzt abgerufen, handelt es sich nicht mehr um Live-Streaming, sondern um ein nicht-lineares On-Demand-Streaming; s.o. Rz. 20 ff.

<sup>342</sup> BRÄNDLI/TAMÒ, sic! 2013, 655; PFORTMÜLLER, SHK URG, Art. 10 N 11; BARRELET/EGLOFF, Art. 10 N 26; REHBINDER/VIGANÒ, Art. 10 N 20.

<sup>343</sup> PFORTMÜLLER, SHK URG, Art. 10 N 11; BARRELET/EGLOFF, Art. 10 N 24 ff.; REHBINDER/VIGANÒ, Art. 10 N 20; das Kriterium der Öffentlichkeit entfällt, falls der Live-Stream nur einem beschränkten Personenkreis i.S.v. Art. 19 Abs. 1 lit. a URG zugänglich gemacht wird.

<sup>344</sup> PFORTMÜLLER, SHK URG, Art. 10 N 11; BARRELET/EGLOFF, Art. 10 N 24 ff.

<sup>345</sup> BOSSHART, 108; PFORTMÜLLER, SHK URG, Art. 10 N 12; WEBER, 271; HILTY, Urheberrecht, Rz. 178; BARRELET/EGLOFF, Art. 10 N 33; REHBINDER/VIGANÒ, Art. 10 N 20; MENN, 98; BÜHLER, 190.



tungsgesellschaften geltend gemacht werden.<sup>346</sup> Die Rechtswahrnehmung ist der Bundesaufsicht unterstellt (Art. 40 Abs. 1 lit. a<sup>bis</sup> URG).

Sobald ein Nutzer ein urheberrechtlich geschütztes Werk, welches über Radio, Fernsehen oder ähnliche Verfahren gesendet wird, als Live-Stream ins Internet stellt, liegt ein „Weitersenden“ i.S.v. Art. 10 Abs. 2 lit. e URG vor.<sup>347</sup>

## B. Schrankenregelung

### a) *Schranke für technisch bedingte Vervielfältigungen ohne eigenständige wirtschaftliche Bedeutung (Art. 24a URG)*<sup>348</sup>

Bei der *Periscope-App* ist bereits das Kriterium der bloss flüchtigen oder begleitenden Vervielfältigung (lit. a) nicht erfüllt, da die hochgeladenen Inhalte während 24 Stunden auf den *Periscope-Servern* abgespeichert werden.<sup>349</sup> Zudem werden die auf den *Servern* hergestellten Kopien nicht nur für die Nutzung der Werke im Rahmen des Live-Streamings hergestellt (lit. b). Diese Vervielfältigungen eröffnen vielmehr weitere Nutzungsmöglichkeiten, indem die hochgeladenen Inhalte während einer bestimmten Zeitspanne auch als On-Demand-Stream konsumiert werden können.

Bei anderen Live-Streaming-Diensten wie etwa *Meerkat* werden nur flüchtige oder begleitende Vervielfältigungen hergestellt, die darüber hinaus einen integralen und wesentlichen Teil des technischen Verfahrens darstellen. Eine Subsumtion dieser Vervielfältigungen unter die Schrankenbestimmung von Art. 24a URG scheitert jedoch an der fehlenden rechtmässigen Nutzung (lit. c) sowie am Merkmal der fehlenden eigenständigen wirtschaftlichen Bedeutung (lit. d). Kopien, die zum Zwecke eines unerlaubten *Uploads* hergestellt werden, sind nicht erlaubt.<sup>350</sup> Ein solch unerlaubter *Upload* liegt etwa vor, wenn urheberrechtlich geschützte Werke ohne Einwilligung der Rechteinhaber im Rahmen des Live-Streaming auf die *Server* der Betreiber hochgeladen und an eine beliebige Zahl Dritter gesendet werden. Sodann kommt diesen Vervielfältigungen auch eine eigenständige wirtschaftliche

---

<sup>346</sup> BOSSHART, 108; OERTLI, SHK URG, Art. 22 N 3 und N 7 ff.; MENN, 98.

<sup>347</sup> BARRELET/EGLOFF, Art. 10 N 33, mit dem Hinweis, dass es sich dabei auch um eine natürliche Person handeln kann; vgl. auch EGLOFF, sic! 2005, 105 f.

<sup>348</sup> Ausführlich dazu Rz. 173 ff.

<sup>349</sup> OERTLI, SHK URG, Art. 24a N 5; JOLLER, 148; BARRELET/EGLOFF, Art. 24a N 4; REHBINDER/VIGANÒ, Art. 24a N 4; s.o. Rz. 147.

<sup>350</sup> OERTLI, SHK URG, Art. 24a N 11.

Bedeutung zu, da sie neue eigenständige Nutzungsmöglichkeiten eröffnen, namentlich den Werkkonsum mittels Live-Streaming.<sup>351</sup>

**b) Schranke des Privatgebrauchs (Art. 19 Abs. 1 lit. a URG)**

- 153 Da der Live-Stream via *Periscope*-, *Meerkat*- oder *YouNow*-App grundsätzlich von einer beliebig grossen Zahl von Nutzern empfangen werden kann, ist die Urheberrechtsschranke zum Privatgebrauch nach Art. 19 Abs. 1 lit. a URG nicht anwendbar.<sup>352</sup>

**C. Urheberstrafrechtliche Konsequenzen**

- 154 Soweit eine Einwilligung der Rechteinhaber fehlt, stellen die transitorischen Vervielfältigungen, die im Rahmen des Live-Streaming auf den *Servern* der Betreiber hergestellt werden, eine unerlaubte Herstellung von Werkexemplaren nach Art. 67 Abs. 1 lit. e URG dar. Wird ein zuvor aufgezeichnetes Werk mittels Live-Stream an eine beliebige Zahl von Personen gesendet, liegt zudem eine unerlaubte Sendung nach Art. 67 lit. h URG vor. Werden die hochgeladenen Daten zugleich auf den *Servern* abgespeichert und einer unbestimmten Anzahl von Personen dergestalt zugänglich gemacht, dass diese von Orten und zu Zeiten ihrer Wahl Zugang haben, ist der Tatbestand der unerlaubten Zugänglichmachung nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG erfüllt. Wenn ein Nutzer ohne Einwilligung der Rechteinhaber ein gesendetes Werk mit einem Aufnahmegerät aufzeichnet und als Live-Stream über das Internet weitersendet, sodass dieses zeitgleich von einer Vielzahl von Personen wahrgenommen werden kann, liegt eine unerlaubte Weitersendung nach Art. 67 lit. h URG vor. Die einzelnen Straftatbestände von Art. 67 URG stehen in echter Konkurrenz zueinander.<sup>353</sup>

---

<sup>351</sup> BARRELET/EGLOFF, Art. 24a N 7.

<sup>352</sup> Eine Werkverwendung im persönlichen Bereich bzw. im Kreis von Personen, die unter sich eng verbunden sind, kommt dann in Betracht, wenn der Stream nur an einige wenige Verwandte oder (enge) Freunde gesendet wird; vgl. Rz. 199.

<sup>353</sup> DAVID, SHK URG, N 13 Vorb. zu Art. 67-73; BARRELET/EGLOFF, Art. 67 N 7; REHBINDER/VIGANÖ, Art. 67 N 7; GLARNER, Musikpiraterie im Internet, 90.

### **3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers**

Dieser Teil der Arbeit ist der rechtlichen Analyse der Nutzerhandlungen beim Streaming gewidmet. Dabei wird eine urheberrechtliche Bewertung der verschiedenen On-Demand-Streaming-Verfahren (*True-On-Demand-Streaming*, *HTTP-Pseudo-Streaming*, *Progressive Download*) aus der Perspektive der Nutzer vorgenommen. Vorab wird der zentralen Frage nachgegangen, ob der Konsum von geschützten Werken mittels Streaming-Verfahren als urheberrechtlich relevante Werknutzung oder bloss als rezeptiver Werkgenuss zu qualifizieren ist. Anschliessend an die rechtliche Qualifikation der einzelnen Vorgänge werden die technischen und rechtlichen Möglichkeiten zum Schutze digitaler Angebote untersucht und eine rechtliche Bewertung möglicher Umgehungshandlungen vorgenommen. 155

#### **I. Urheberrechtlich relevante Werknutzung oder bloss rezeptiver Werkgenuss?**

Die Übertragung digitaler Inhalte mittels Streaming-Verfahren setzt voraus, 156 dass die digitalen Inhalte vom *Server* zunächst in einzelne Datenpakete zerlegt und sodann kontinuierlich ins Datennetz eingespeist werden.<sup>354</sup> Um Schwankungen in der Datenübertragung auszugleichen und eine flüssige Wiedergabe des Werks zu gewährleisten, werden auf dem Nutzerrechner jeweils einige Sekunden der empfangenen Inhalte in einem sog. Puffer zwischengespeichert.<sup>355</sup> Sodann finden weitere (vorübergehende) Vervielfältigungen bei der anschliessenden computergestützten Werkwiedergabe auf dem Nutzerrechner statt.<sup>356</sup> Folglich muss geklärt werden, ob die vorübergehenden Vervielfältigungen, die im Rahmen des Streamings hergestellt werden, überhaupt eine rechtlich relevante Werknutzung darstellen, oder ob von einem bloss rezeptiven Werkgenuss auszugehen ist. Diese Unterscheidung ist bedeutsam, da der blosser Werkgenuss nicht gestützt auf das Urheberrecht untersagt werden

---

<sup>354</sup> HILGERT/GRETH, 105 f.; EICHELBERGER, 30; OĞLAKCIOĞLU, ZIS 2012, 433.

<sup>355</sup> KUROSE/ROSS, 628 f.; EICHELBERGER, 30; TANENBAUM/WETHERALL, 808 ff.

<sup>356</sup> BORNHAUSER, Rz. 364; WANDTKE/VON GERLACH, GRUR 2013, 677.

kann.<sup>357</sup> Reiner Werkgenuss wird von der Lehre als reiner Genuss mit den Sinnen definiert, wie dies bspw. beim Musikhören, beim Lesen eines Buches, beim Betrachten eines Bildes oder beim Anschauen eines Filmes geschieht.<sup>358</sup>

- 157 Beim Streaming ist zu differenzieren zwischen dem Vorgang der sinnlichen Wahrnehmung des Werks durch den Konsumenten und den technisch bedingten Vervielfältigungen, die bei der computerunterstützten Nutzung digitaler Inhalte innerhalb des Nutzerrechners hergestellt werden.<sup>359</sup> Das sinnliche Wahrnehmen eines Werks (am Bildschirm, über Lautsprecher etc.) ist ein rein rezeptiver Werkgenuss.<sup>360</sup> Bei den technisch bedingten Teilervielfältigungen, die im Rahmen des Streaming auf dem Nutzerrechner hergestellt werden, stellt sich die Frage, ob diese als rechtlich relevante Vervielfältigungen i.S.v. Art. 10 Abs. 2 lit. a URG zu qualifizieren sind. Letztgenannte Bestimmung verleiht dem Urheber das ausschliessliche Recht, Werkexemplare wie Druckerzeugnisse, Ton-, Tonbild oder Datenträger herzustellen. Der Begriff der Vervielfältigung ist dabei weit auszulegen. Gemäss herrschender Lehre in der Schweiz werden – ungeachtet ihres transitorischen Charakters – sämtliche körperlichen wie auch unkörperlichen Vervielfältigungen von Art. 10 Abs. 2 lit. a URG erfasst, sofern eine minimale Dauerhaftigkeit gegeben ist.<sup>361</sup>
- 158 Ob bereits ein einzelnes zwischengespeichertes Fragment die vom Urheberrecht geforderte Schöpfungshöhe erreicht, um das Vorliegen einer geistigen Schöpfung mit individuellem Charakter zu bejahen, hängt vom Umfang der Zwischenspeicherung ab.<sup>362</sup> Nachfolgend wird untersucht, ob die beim Streaming anfallenden transitorischen Teilervielfältigungen als rechtlich relevante Vervielfältigung i.S.v. Art. 10 Abs. 2 lit. a URG zu qualifizieren sind.<sup>363</sup> Richtigerweise kommt es dabei auf sämtliche Zwischenspeicherungen an, die

---

<sup>357</sup> PFORTMÜLLER, SHK URG, Art. 10 N 2; HILTY, Urheberrecht, Rz. 150.

<sup>358</sup> BORNHAUSER, Rz. 172 ff.; BARRELET/EGLOFF, Art. 10 N 6a; GASSER, 40 f.; zum deutschen Recht MARLY, EuZW 2014, 617.

<sup>359</sup> BRÄNDLI/TAMÒ, sic! 2013, 657; KUROSE/ROSS, 628; TANENBAUM/WETHERALL, 813 f.,

<sup>360</sup> BRÄNDLI/TAMÒ, sic! 2013, 657; HILTY, Urheberrecht, Rz. 156 und 175; BAUMGARTNER, 41.

<sup>361</sup> BRÄNDLI/TAMÒ, sic! 2013, 657; OERTLI, SHK URG, Art. 24a N 2; BARRELET/EGLOFF, Art. 10 N 12; HÄUPLI, 176 f.; BERGER, sic! 2002, 670; DESSEMONTET, droit d'auteur, 170 f; HILTY, sic! 1997, 135 f; FRÖHLICH-BLEULER, AJP 1995, 571; a.A. BÜHLER, 149 ff. und 168.

<sup>362</sup> BRÄNDLI/TAMÒ, sic! 2013, 657; WANDTKE/VON GERLACH, GRUR 2013, 677; BARRELET/EGLOFF, Art. 2 N 27; ZECH, ZUM 2014, 6.

<sup>363</sup> BRÄNDLI/TAMÒ, sic! 2013, 657; WANDTKE/VON GERLACH, GRUR 2013, 677.

beim Streaming-Vorgang innerhalb des Nutzerrechners hergestellt werden.<sup>364</sup> Dabei sind sowohl der Umfang als auch die Bestandsdauer der Teilvervielfältigung entscheidend.<sup>365</sup>

## 1. Umfang der Teilvervielfältigung

In Abhängigkeit von den zur Übertragung eingesetzten *Servern* (*Web-Server* 159 oder *Streaming-Server*) und dem dazugehörigen Transportprotokoll (*TCP* oder *UDP*), fällt der Umfang der Vervielfältigungen unterschiedlich aus.<sup>366</sup>

Beim Streaming von einem **Web-Server** mit Einsatz des *TCP*-Protokolls 160 werden beim Abspielen einer Audio-Video Datei gewöhnlich folgende Teilvervielfältigungen auf dem Nutzerrechner hergestellt<sup>367</sup>:

- im *TCP-Empfangspuffer* (weniger als zwei Sekunden bei der Wiedergabe von Audio-/Video-Inhalten<sup>368</sup>)
- im *Client-Puffer* (zwei bis fünf Sekunden bei Audio-/Video-Inhalten<sup>369</sup>)
- im Prozessorspeicher (0,00079 Sekunden bei der Wiedergabe von Audio Inhalten bzw. 0,00018 Sekunden bei der Wiedergabe von Audio-/Video-Inhalten<sup>370</sup>)
- im Audio-/Video-Speicher (vier Sekunden bei der Wiedergabe einer MP3-Datei bzw. 0,12 Sekunden bei Videodateien<sup>371</sup>)

---

<sup>364</sup> WANDTKE/VON GERLACH, GRUR 2013, 677, im Normalfall fallen Zwischenspeicherungen im *TCP-Empfangspuffer*, im *Client-Puffer*, im Prozessorspeicher, im Audio/Video-Speicher und im *Cache-Speicher* an.

<sup>365</sup> BRÄNDLI/TAMÒ, sic! 2013, 657; WANDTKE/VON GERLACH, GRUR 2013, 677.

<sup>366</sup> HILGERT/GRETH, 106; KUROSE/ROSS, 630 ff.; WANDTKE/VON GERLACH, GRUR 2013, 677; BRÄNDLI/TAMÒ, sic! 2013, 653; STOLZ, MMR 2013, 354; STIEPER, MMR 2012, 13.

<sup>367</sup> Ausführlich WANDTKE/VON GERLACH, GRUR 2013, 676 ff.; VON GERLACH, 113 ff., m.w.H.; STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 497.

<sup>368</sup> VON GERLACH, 74.

<sup>369</sup> MAY, 168; KUROSE/ROSS, 632 f.; WANDTKE/VON GERLACH, GRUR 2013, 677; TANENBAUM/WETHERALL, 813 f., geben sogar 5-10 Sekunden als Referenzwert für die Pufferung der Mediendaten, bevor sie mit der Wiedergabe beginnen; STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 497 f.

<sup>370</sup> WANDTKE/VON GERLACH, GRUR 2013, 677.

<sup>371</sup> WANDTKE/VON GERLACH, GRUR 2013, 677.

3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers

---

- Im *Cache-Speicher* (beim Progressiven Download und beim http-Pseudo-Streaming liegt am Ende der Wiedergabe eine komplette Zwischenspeicherung der wiedergegebenen Audio-/Video-Inhalte<sup>372</sup> vor)

<sup>161</sup> Wird ein **Streaming-Server** sowie das verbindungslose *UDP-Protokoll* eingesetzt, werden im *UDP-Empfangspuffer* Teilervielfältigungen im Umfang von 0,09 Sekunden beim Abspielen einer *MP3*-Datei bzw. 0,02 Sekunden bei der Wiedergabe einer Videodatei hergestellt. Aufgrund der Echtzeitkommunikation entfällt eine vollständige Zwischenspeicherung der gestreamten Datei im *Cache-Speicher*. Hinsichtlich des Umfanges der übrigen Speichervorgänge kann auf die zuvor gemachten Ausführungen zum Streaming von einem Web-Server verwiesen werden.<sup>373</sup>

## 2. Bestandsdauer der Teilervielfältigung

<sup>162</sup> Damit eine urheberrechtlich relevante Vervielfältigung i.S.v. Art. 10 Abs. 2 lit. a URG vorliegt, muss diese eine gewisse minimale Dauerhaftigkeit aufweisen. Nachfolgende Ausführungen betreffen die Bestandsdauer, während der die Teilervielfältigungen auf dem Nutzerrechner zwischengespeichert sind<sup>374</sup>:

- Die Teilervielfältigungen im *TCP/UDP-Empfangspuffer* werden nach dem Verschieben in den *Client-Puffer* gelöscht.
- Nach erfolgter Wiedergabe werden die Teilervielfältigungen im *Client-Puffer* in den *Cache-Speicher* verschoben und so aus dem Hauptspeicher gelöscht.<sup>375</sup>
- Teilervielfältigungen im Prozessorspeicher werden durch die nächste atomare Rechenoperation gelöscht.<sup>376</sup>

---

<sup>372</sup> GALETZKA/STAMER, MMR 2014, 296 ff.; MAY, 168; ENSTHALER, NJW 2014, 1553; WANDTKE/VON GERLACH, GRUR 2013, 677; VON GERLACH, 82; LONGOLIUS, 47 ff.; STOLZ, MMR 2013, 356; BUSCH, GRUR 2011, 501.

<sup>373</sup> Zum Ganzen WANDTKE/VON GERLACH, GRUR 2013, 677; VON GERLACH, 43 f. und 82 f.; LONGOLIUS, 49 f.

<sup>374</sup> MAY, 168; ENSTHALER, NJW 2014, 1553 f.; WANDTKE/VON GERLACH, GRUR 2013, 677; VON GERLACH, 57 ff.; STOLZ, MMR 2013, 354; BUSCH, GRUR 2011, 498.

<sup>375</sup> GALETZKA/STAMER, MMR 2014, 296; WANDTKE/VON GERLACH, GRUR 2013, 677; BUSCH, GRUR 2011, 501; BORGHI, IIC 2011, 328.

- Die Teilvervielfältigungen im Audio-/Video-Speicher werden nach erfolgter Wiedergabe auf dem Nutzerrechner durch neue Audio-/Video-Daten überschrieben.<sup>377</sup>
- Die Vervielfältigungen im *Cache*-Speicher (beim progressiven Download und beim HTTP-Pseudo-Streaming von einem **Web-Server**) werden durch das Schliessen des Media-Players automatisch gelöscht bzw. mit neuen Daten überschrieben.<sup>378</sup> Im Gegensatz dazu werden beim *True-On-Demand-Streaming* von einem **Streaming-Server** die Teilvervielfältigungen unmittelbar nach der Wiedergabe im Media-Player vernichtet.<sup>379</sup>

### 3. Schutzfähigkeit von Teilvervielfältigungen

WANDTKE/VON GERLACH zeigen in ihrer technischen Analyse auf, dass die 163 zwischengespeicherten Teile beim Streaming im technischen Regelfall „ein Minimum an künstlerischer Gestaltung aufweisen“ (Zwischenspeicherungen im *TCP-Empfangspuffer*) bzw. sogar „individuelle Züge der Urheber wiedergeben und damit erst recht individualisierbar sind“ (Zwischenspeicherungen im *Client-Puffer*).<sup>380</sup> Da es sich hierbei stets um Einzelfallbetrachtungen handelt, ist der Nachweis der Schutzfähigkeit der Teilvervielfältigungen mit praktischen Hindernissen behaftet: Erstens kann rückblickend nicht festgestellt werden ob die einzelnen Segmente schutzwürdig waren, da diese in der Regel bereits während der Wiedergabe wieder überschrieben werden. Zweitens ist es angesichts der riesigen Vielzahl einzelner Segmente nicht möglich, diese auf ihre jeweilige Schöpfungshöhe hin zu überprüfen.<sup>381</sup> VON GERLACH kritisiert, dass es von technischen Zufällen, Ausnahmen oder dem technischen Fort-

---

<sup>376</sup> WANDTKE/VON GERLACH, GRUR 2013, 677; BUSCH, GRUR 2011, 501.

<sup>377</sup> GALETZKA/STAMER, MMR 2014, 296; WANDTKE/VON GERLACH, GRUR 2013, 677; BUSCH, GRUR 2011, 501.

<sup>378</sup> HILGERT/GRETH, 106; STIEPER, MMR 2012, 13.

<sup>379</sup> HILGERT/HILGERT, MMR 2014, 86; GALETZKA/STAMER, MMR 2014, 296; WANDTKE/VON GERLACH, GRUR 2013, 677; STOLZ, MMR 2013, 355; JANISCH/LACHENMANN, MMR 2013, 213; STIEPER, MMR 2012, 15; BUSCH, GRUR 2011, 501; RADMANN, ZUM 2010, 388; KOCH, GRUR 2010, 574 f.

<sup>380</sup> WANDTKE/VON GERLACH, GRUR 2013, 678.

<sup>381</sup> Vgl. MAY, 174; ENSTHALER, NJW 2014, 1554; GALETZKA/STAMER, MMR 2014, 294 ff.; WANDTKE/VON GERLACH, GRUR 2013, 678; VON GERLACH, 113 ff.; STOLZ, MMR 2013, 355; STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 499.

schritt abhängig sei, ob eine rechtlich relevante Vervielfältigung vorliegt oder nicht.<sup>382</sup>

- 164 Um dieser Problematik beizukommen wird von Vertretern in der deutschen Lehre vorgeschlagen, dass nicht auf die Schutzfähigkeit des konkret zwischengespeicherten Werkteils abgestellt, sondern von einem normativen Vervielfältigungsbegriff ausgegangen werden sollte: *„Als Vervielfältigung aufgefasst werden muss danach auch die sukzessive, chronologisch geordnete, auch nur flüchtige Vervielfältigung von an sich nicht schutzfähigen Werkteilen, solange in der Gesamtbetrachtung das ganze Werk oder schutzfähige Teile davon vervielfältigt werden“*<sup>383, 384</sup>

---

<sup>382</sup> WANDTKE/VON GERLACH, GRUR 2013, 683; VON GERLACH, 203 ff.; ebenso ENSTHALER, NJW 2014, 1554; SCHULZE, NJW 2014, 722; STOLZ, MMR 2013, 355; VIANELLO, CR 2010, 729.

<sup>383</sup> STOLZ, MMR 2013, 355.

<sup>384</sup> Gl. M. ENSTHALER, NJW 2014, 1554, m.w.H.; WANDTKE/VON GERLACH, GRUR 2013, 683, die von einem „sequentiellen Vervielfältigungsbegriff“ sprechen und vorschlagen, das Vervielfältigungsrecht *de lege ferenda* dahingehend abzuändern, dass „die Gesamtheit der sukzessiv zwischengespeicherten, an sich nicht schutzfähigen Teile schutzfähiger Audio-Video Inhalte oder eines Teils davon“ ausschlaggebend sein soll; VON GERLACH, 212 ff.; OĞLAKCIOĞLU, ZIS 2012, 436; FANGEROW/SCHULZ, GRUR 2010, 678; a.A. MAY, 172, wendet ein, dass eine Zwischenspeicherung auf dem PC „niemals gänzlich geordnet oder als zusammenhängendes Werk erfolgt“, SCHEDER-BIESCHIN, 167 f., der darauf verweist, dass Art. 2 lit. a) der Info-Richtlinie unionsweit einheitlich auszulegen ist und dieser nach Ansicht des EuGH nicht den gesamten Stream, sondern nur die „zu einem bestimmten Zeitpunkt vorhandenen [...] Fragmente“ umfasst; BUSCH, GRUR 2011, 496 ff.; kritisch GALETZKA/STAMER, MMR 2014, 294 f., die aber mit Verweis auf den EuGH, Urteil vom 4. Oktober 2011, Rechtssache C-403/08, FAPL/Murphy, zum Schluss kommen, dass für eine Gegenmeinung, zumindest in der beratenden Praxis, kein Raum mehr besteht und so auch Speicherungen im Arbeitsspeicher als rechtlich relevante Vervielfältigungen zu qualifizieren seien. Mit Blick auf Teilvervielfältigungen soll eine relevante Vervielfältigung aber erst dann ohne Weiteres angenommen werden, wenn der gespeicherte Teil für sich genommen schutzfähig ist. Da im Einzelfall – wie die Autoren dies selbst auch einräumen – die Länge und der Umfang der zwischengespeicherten Sequenzen praktisch nie festgestellt werden kann, ist die von diesen Autoren vorgeschlagene Einschränkung m.E. abzulehnen und auf die Gesamtheit der sukzessiv zwischengespeicherten Daten abzustellen; STIEPER, MMR 2012, 13 f., argumentiert, dass „nicht der Umfang der jeweils nur flüchtigen Zwischenspeicherungen, sondern der Umfang der dadurch ermöglichten Werknutzung über das Vorliegen einer urheberrechtlich relevanten Vervielfältigung entscheiden müsse“, wendet aber sogleich ein, dass diese Auslegung nicht mit Art. 2 Info-Richtlinie vereinbar wäre, falls eine „sequenzielle Speicherung an sich nicht schutzfähiger Werkteile“ als Vervielfältigung qualifiziert würde.



MAY kritisiert an dieser Ansicht, dass die einzelnen Filmfragmente nicht immer in chronologisch geordneter Reihenfolge übertragen sowie eine chronologische Ordnung der Werkteile erst durch die Abspiel-Software erfolgen würde. Zudem würde das übermittelte Werk auf dem Nutzerrechner nicht gänzlich geordnet, sondern aufgesplittert in kleine Werkteile, abgespeichert.<sup>385</sup> Dagegen lässt sich einwenden, dass es nicht darauf ankommen kann, in welcher Reihenfolge die einzelnen Fragmente auf dem Empfangsgerät ankommen und wo diese zwischengespeichert werden. Vielmehr sollte einzig der Umstand entscheidend sein, dass die zwischengespeicherten Fragmente durch Verwendung einer geeigneten Abspielsoftware in eine chronologische Reihenfolge gebracht und wiedergegeben werden können. 165

Die Bestimmung von Art. 10 Abs. 2 lit. a URG macht – wie HILTY richtig bemerkt – einen „antiquierten Eindruck“, indem noch beispielhaft die Herstellung von Druckerzeugnissen aufgeführt wird, obschon das Druckverfahren bereits seit Jahrzehnten durch modernere Kopierverfahren abgelöst worden ist.<sup>386</sup> Mit Blick auf die veränderten technischen Gegebenheiten und die Rechtssicherheit wäre eine Anpassung dieser Norm angezeigt. Aus dem Wortlaut der revidierten Bestimmung sollte klar hervorgehen, dass sämtliche – auch bloss transitorischen Vervielfältigungen – vom Vervielfältigungsrecht erfasst werden, solange in einer Gesamtbetrachtung sukzessive das Werk oder schutzfähige Teile davon vervielfältigt werden.<sup>387</sup> 166

Ein anderer Ansatz leitet im Umkehrschluss aus Art. 24a URG ab, dass „bereits die vorübergehende Vervielfältigung im Arbeitsspeicher urheberrechtliche Relevanz entfaltet“<sup>388</sup>. Falls vorübergehende Vervielfältigungen unter den rezeptiven Werkgenuss subsumiert würden, wäre die Bestimmung von Art. 24a URG überflüssig, da der rezeptive Werkgenuss ohnehin keiner Zustimmung des Urhebers bedarf.<sup>389</sup> 167

---

<sup>385</sup> MAY, 171 f., m.w.H.

<sup>386</sup> HILTY, Urheberrecht, Rz. 156.

<sup>387</sup> A.A. BORNHAUSER, Rz. 172 ff., der bei Zwischenspeicherungen im Arbeitsspeicher von Digitalrechnern eine Vervielfältigung i.S.v. Art. 10 Abs. 2 lit. a URG verneint und dies damit begründet, dass diese „vielmehr grundlegende Voraussetzung für das Funktionieren von Digitalrechnern [sind] und deshalb im Verhältnis zum Genuss digitaler Werke mittels Digitalrechnern bloss akzessorischer Natur [sind]“.

<sup>388</sup> HILTY, Urheberrecht, Rz. 156.

<sup>389</sup> BRÄNDLI/TAMÖ, sic! 2013, 657 f., mit dem Hinweis, dass ansonsten die Schaffung einer gesetzlichen Schrankenregelung für flüchtige Vervielfältigungen überflüssig gewesen wäre; HÄUPTLI, 176 f.

- 168 Zusammenfassend kann festgehalten werden, dass sowohl beim On-Demand-Streaming von einem *Streaming-Server* als auch bei jenem von einem *Web-Server* transitorische Teilvervielfältigungen der Inhalte, oder zumindest eines winzigen Segments davon, stattfinden.<sup>390</sup> Damit das Vorliegen einer rechtlich relevanten Vervielfältigung gem. Art. 10 Abs. 2 lit. a URG nicht von technischen Zufällen abhängt, sollte für die Bewertung die Gesamtheit der sukzessive zwischengespeicherten Werkteile massgebend sein.<sup>391</sup>
- 169 Die bei der Werkwiedergabe mittels Streaming hergestellten, flüchtigen Vervielfältigungen können zudem einen Eingriff in das Vervielfältigungsrecht der Hersteller von Ton- und Tonbildträgern darstellen (Art. 36 lit. a URG).<sup>392</sup> Geschützt wird durch diese Bestimmung gemäss der Botschaft von 1989 „*der komplexe Produktionsvorgang, der einem Ton- oder Tonbildträger zugrunde liegt und auf einer qualifizierten unternehmerischen Leistung beruht*“<sup>393</sup>. Das Vervielfältigungsrecht der Hersteller umfasst auch die Vervielfältigung bloss von Teilen des Ton- oder Tonbildträgers.<sup>394</sup>
- 170 Mit Blick auf die deutsche Rechtsprechung ist ein Urteil des BGH interessant, in welchem dieser festhielt, dass ein Eingriff in das Vervielfältigungsrecht unabhängig sei von der Quantität oder Qualität des übernommenen Abschnitts, da die für die Aufnahme erforderlichen Mittel für den kleinsten Teil der Aufnahme genauso bereitgestellt werden müssten wie für die gesamte Aufnahme.<sup>395</sup> Dies hat zur Konsequenz, dass bereits die Vervielfältigung jedes noch so kleinen Werkteils vom Vervielfältigungsrecht der Hersteller von Ton- und Tonbildträgern erfasst wird.<sup>396</sup> Daraus folgert EICHELBERGER, dass bei technisch bedingten Teilvervielfältigungen beim Streaming stets ein

---

<sup>390</sup> CHERPILLOD, SIWR II/1, 290; BRUNOTTE, 16; STOLZ, MMR 2013, 355, der zutreffend darauf hinweist, dass lediglich die Intensität der Speicherung bei den verschiedenen Streaming-Verfahren und Einstellungsmöglichkeiten variiert; BUSCH, GRUR 2011, 496 ff.; RADMANN, ZUM 2010, 387 f.

<sup>391</sup> WANDTKE/VON GERLACH, GRUR 2013, 683; VON GERLACH, 212 ff.; STOLZ, MMR 2013, 355; STIEPER, MMR 2012, 13 f.; FANGEROW/SCHULZ, GRUR 2010, 678; a.A. MAY, 172; SCHEDER-BIESCHIN, 167; BUSCH, GRUR 2011, 496 ff.

<sup>392</sup> AUF DER MAUR, SHK URG, Art. 36 N 11.

<sup>393</sup> Botschaft URG 1989, 550.

<sup>394</sup> AUF DER MAUR, SHK URG, Art. 36 N 11; BARRELET/EGLOFF, Art. 36 N 8; REHBINDER/VIGANÒ, Art. 36 N 3.

<sup>395</sup> BGH, Az. I ZR 112/06, GRUR 2009, 404; EICHELBERGER, 33.

<sup>396</sup> EICHELBERGER, 33.

Eingriff in das Vervielfältigungsrecht des Tonträger-, Film- bzw. Laufbildherstellers vorliegt.<sup>397</sup>

Soweit ersichtlich existiert für die Schweiz noch keine abschliessende 171  
höchstrichterliche Rechtsprechung zur Frage nach der Schutzfähigkeit  
kleinster Teilvervielfältigungen im Kontext zu dem in Art. 36 lit. a URG  
statuierten Vervielfältigungsrecht. Damit die Hersteller von Ton- oder Ton-  
bildträgern bei Vervielfältigungshandlungen keinen stärkeren Schutz durch  
das Urheberrecht geniessen als die Urheber selbst, sollte auch hier der Um-  
stand entscheidend sein, ob bei einer Gesamtbetrachtung sämtlicher Spei-  
chervorgänge, die im Rahmen des Streaming stattfinden, das Werk bzw.  
schutzfähige Teile davon vervielfältigt werden.<sup>398</sup>

## II. Schranken des Urheberrechts

Die Schrankenregelungen im Urheberrecht sollen einen Ausgleich zwischen 172  
den divergierenden Interessen der Rechteinhaber und der Werknutzer ermög-  
lichen, indem die ausschliesslichen Rechte der Urheber an ihren Werken  
durch einzelne Bestimmungen zugunsten der Nutzer eingeschränkt wer-  
den.<sup>399</sup> Die beim Streaming anfallenden transitorischen Vervielfältigungen  
sind richtigerweise als rechtlich relevante Werknutzungen i.S.v. Art. 10  
Abs. 2 lit. a URG, Art. 33 Abs. 2 lit. c URG, Art. 36 lit. a URG bzw. Art. 37  
lit. c URG zu qualifizieren.<sup>400</sup> Soweit die Nutzung der geschützten Werke  
mittels Streaming mit der Einwilligung der Rechteinhaber vertraglich gere-  
gelt wurde, bedarf es keiner Schrankenbestimmung.<sup>401</sup> Demgegenüber muss  
bei der Nutzung nicht-lizenzierter Streaming-Angebote geprüft werden, ob  
die dabei hergestellten flüchtigen Vervielfältigungen durch die Schranke für  
ausschliesslich technisch bedingte Kopien ohne eigenständige wirtschaftli-

---

<sup>397</sup> EICHELBERGER, 33 f.; gl. M. MAY, 175.

<sup>398</sup> S.o. Rz. 163 f.

<sup>399</sup> Urteil 4A\_295/2014 des Bundesgerichts vom 28. November 2014, Erw. 3.6.2.;  
GASSER/OERTLI, SHK URG, N 1 ff. Vorb. zum 5. Kapitel; GIRSBERGER, 190; BÜHLER,  
253.

<sup>400</sup> Vgl. Rz. 163 ff.

<sup>401</sup> BRÄNDLI/TAMÖ, sic! 2013, 658 f.

che Bedeutung nach Art. 24a URG oder eine andere Schranke des Urheberrechts gedeckt sind.<sup>402</sup>

## **1. Schranke für technisch bedingte Vervielfältigungen ohne eigenständige wirtschaftliche Bedeutung (Art. 24a URG)**

- <sup>173</sup> Da bei der computerbasierten Nutzung digitaler Werke ausnahmslos vorübergehende Vervielfältigungen hergestellt werden, führte das in Art. 10 Abs. 2 lit. a URG geregelte Vervielfältigungsrecht zu praxisfremden Ergebnissen.<sup>403</sup> Technisch bedingte, transitorische Speicherungen – wie sie etwa beim Streaming anfallen – waren ausserhalb des privaten Gebrauchs nach Art. 19 Abs. 1 lit. a URG eigentlich unzulässig.<sup>404</sup> Dieser Umstand sollte im Zuge der URG-Revision von 2007 korrigiert werden.<sup>405</sup> Mit Art. 24a URG wurde neu eine umfassende Schranke für flüchtige oder begleitende Vervielfältigungen ohne eigenständige wirtschaftliche Bedeutung eingeführt. Vorausgesetzt wird, dass die Kopie nur einen flüchtigen oder begleitenden Charakter hat (lit. a), einen integralen und wesentlichen Teil eines technischen Verfahrens darstellt (lit. b), ausschliesslich der Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder einer rechtmässigen Nutzung dient (lit. c) sowie keine eigenständige wirtschaftliche Bedeutung hat (lit. d).<sup>406</sup> Die einzelnen Tatbestandsvoraussetzungen (lit. a-d) müssen kumulativ erfüllt sein.<sup>407</sup>

---

<sup>402</sup> Vgl. auch RUBLI, Rz. 60, welcher die Meinung vertritt, dass Art. 24a URG zwar als Schrankenbestimmung konzipiert sei, es sich dabei aber um eine Reduktion der Tatbestandsmässigkeit einer Vervielfältigung handeln würde.

<sup>403</sup> OERTLI, SHK URG, Art. 24a N 1; HILTY, Urheberrecht, Rz. 229; BORNHAUSER, Rz. 97 ff.; BARRELET/EGLOFF, Art. 24a N 1.

<sup>404</sup> OERTLI, SHK URG, Art. 24a N 1; JOLLER, 147 ff.; GILLIÉRON, sic! 2009, 763; BARRELET/EGLOFF, Art. 10 N 12 und Art. 24a N 1; REHBINDER/VIGANÒ, Art. 24a N 1; BERGER, sic! 2002, 670; HILTY, sic! 2004, 973.

<sup>405</sup> BARRELET/EGLOFF, Art. 24a N 1; RUBLI, Rz. 58 ff.

<sup>406</sup> OERTLI, SHK URG, Art. 24a N 3; BARRELET/EGLOFF, Art. 24a N 1; REHBINDER/VIGANÒ, Art. 24a N 2; HILTY, Urheberrecht, Rz. 229, der die Frage aufwirft, ob es sich bei dieser Bestimmung um eine Schrankenregelung handelt oder nicht eher um eine Bereichsausnahme zur Einschränkung des umfassenden Vervielfältigungsbegriffs von Art. 10 Abs. 2 lit. a URG; Botschaft URG 2006, 3431.

<sup>407</sup> BRÄNDLI/TAMÒ, sic! 2013, 658 f.; OERTLI, SHK URG, Art. 24a N 4; BARRELET/EGLOFF, Art. 24a N 3; REHBINDER/VIGANÒ, Art. 24a N 3; Botschaft URG 2006, 3430 f.

### A. Vorübergehende flüchtige oder begleitende Vervielfältigung (lit. a)

Eine Vervielfältigung ist *flüchtig*, wenn es sich um eine besonders kurzlebige, 174 rasch vergängliche Kopie handelt, die spätestens mit der Beendigung des Abspielvorgangs oder einem Unterbruch der Stromzufuhr wieder gelöscht wird.<sup>408</sup> Das Erfordernis einer *begleitenden* Vervielfältigung ist erfüllt, wenn diese bloss zur Erleichterung eines anderen Nutzungsvorganges dient.<sup>409</sup>

Beim *True-On-Demand-Streaming* ist das Vorliegen einer bloss flüchtigen 175 Vervielfältigung ohne Weiteres zu bejahen, da die Kopie in der Regel bereits nach kurzer Zeit wieder gelöscht wird (Echtzeitkommunikation).<sup>410</sup>

Werden im Rahmen des *HTTP-Pseudo-Streaming* temporäre Vervielfältigungen 176 angefertigt, die spätestens mit dem Schliessen des *Browsers* oder dem Herunterfahren des Systems wieder gelöscht werden, sollte dies der Annahme einer flüchtigen Vervielfältigung nicht entgegenstehen.<sup>411</sup> Der Durchschnittsnutzer wird die unterschiedlichen internen Speichervorgänge kaum bemerken, geschweige denn in der Lage sein, diese temporären Vervielfältigungen für anderweitige Nutzungen zu verwenden.<sup>412</sup> Betrachtet man die audiovisuelle Wahrnehmung des Streams als den eigentlichen Hauptzweck, ist sowohl beim *True-On-Demand-Streaming* wie auch beim *HTTP-Pseudo-Streaming* das Kriterium der begleitenden Vervielfältigung erfüllt, da die Zwischenspeicherungen bloss beiläufig im Rahmen des technischen Wiedergabeverfahrens hergestellt werden.<sup>413</sup>

<sup>408</sup> OERTLI, SHK URG, Art. 24a N 5; BARRELET/EGLOFF, Art. 24a N 4; REHBINDER/VIGANÒ, Art. 24a N 4.

<sup>409</sup> OERTLI, SHK URG, Art. 24a N 6, weist darauf hin, dass Kopien, die bei der normalen Internetnutzung beim „Browsing“ oder „Caching“ anfallen, als begleitende Vervielfältigungen i.S.v. Art. 24a lit. a URG zu qualifizieren sind; JOLLER, 148; BARRELET/EGLOFF, Art. 24a N 4; REHBINDER/VIGANÒ, Art. 24a N 5, lassen genügen, wenn die Vervielfältigung massgebend zum effizienten Funktionieren der Übertragungssysteme beitragen; BGE 133 III 473, Erw. 4.4; Botschaft URG 2006, 3402.

<sup>410</sup> BRÄNDLI/TAMÒ, sic! 2013, 658; LONGOLIUS, 49 f.

<sup>411</sup> OERTLI, SHK URG, Art. 24a N 5 f., mit Verweis auf die Tatsache, dass auch Caching-Kopien regelmässig während längerer Zeit bestehen bleiben und dieser Umstand das Kriterium der flüchtigen Vervielfältigung nicht verletzt; REHBINDER/VIGANÒ, Art. 24a N 4; BUSCH, GRUR 2011, 501; LONGOLIUS, 47 ff.

<sup>412</sup> BUSCH, GRUR 2011, 502; LONGOLIUS, 47 ff.

<sup>413</sup> BRÄNDLI/TAMÒ, sic! 2013, 658; REHBINDER/VIGANÒ, Art. 24a N 4; BARRELET/EGLOFF, Art. 24a N 4.

- 177 Anders zu beurteilen ist die Rechtslage bei einem *Progressive Download* mit dauerhafter Speicherung.<sup>414</sup> Vergleichbar mit der Situation beim klassischen Download wird das gesamte Werk heruntergeladen und auf dem Nutzerrechner abgespeichert. Das Tatbestandserfordernis der bloss flüchtigen Vervielfältigung ist somit nicht erfüllt.<sup>415</sup> Auch das Vorliegen einer bloss begleitenden Vervielfältigung muss verneint werden, weil diese nicht bloss beiläufig (technisch bedingt) während des Streaming-Vorgangs entsteht, sondern gezielt angefertigt wird, um einen späteren Abruf der Datei auch offline zu ermöglichen.<sup>416</sup>

## **B. Die Vervielfältigung ist integraler und wesentlicher Teil eines technischen Verfahrens (lit. b)**

- 178 Negativ ausgedrückt ist eine Vervielfältigung immer dann als *integraler und wesentlicher Bestandteil eines technischen Verfahrens* anzusehen, wenn sie nicht als gezielte bzw. zumindest erwünschte Umgehung des Vervielfältigungsverbots erscheint.<sup>417</sup>
- 179 Das *True-On-Demand-Streaming* sowie das *HTTP-Pseudo-Streaming* erfüllen diese Voraussetzungen zweifellos, da die vorübergehenden Vervielfältigungen zwingend erforderlich sind, um Schwankungen bei der Übertragungsrate (*Jitter*<sup>418</sup>) auszugleichen und ein störungsfreies Abspielen der Audio-/Video-Dateien zu gewährleisten.<sup>419</sup>
- 180 Demgegenüber wird beim *Progressive Download* mit dauerhafter Speicherung gezielt eine Kopie des Werks hergestellt, die nicht bloss der Wiedergabe des

---

<sup>414</sup> HILGERT/GRETH, 106, weisen darauf hin, dass beim *Progressiven Download* die in Sequenzen übertragenen Werkfragmente als sog. temp-Datei gespeichert wird, „so dass die Vervielfältigung des gesamten Werks selbst dann vorliegt, wenn diese Datei unmittelbar nach der Wiedergabe gelöscht wird“; STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 501.

<sup>415</sup> GALETZKA/STAMER, MMR 2014, 296; HILGERT/HILGERT, MMR 2014, 86.

<sup>416</sup> HILGERT/GRETH, 108; STIEPER, MMR 2012, 15.

<sup>417</sup> OERTLI, SHK URG, Art. 24a N 8; BARRELET/EGLOFF, Art. 24a N 5; REHBINDER/VIGANÒ, Art. 24a N 5.

<sup>418</sup> KUROSE/ROSS, 650; TANENBAUM/WETHERALL, 625 ff., 814.

<sup>419</sup> HILGERT/GRETH, 109; GALETZKA/STAMER, MMR 2014, 296; WANDTKE/VON GERLACH, GRUR 2013, 679; STOLZ, MMR 2013, 356; STIEPER, MMR 2012, 15; EICHELBERGER, 31; BUSCH, GRUR 2011, 501; FANGEROW/SCHULZ, GRUR 2010, 680; RADMANN, ZUM 2010, 390.

Werks dient.<sup>420</sup> Eine dauerhafte Vervielfältigung ist für ein reibungsloses Funktionieren des Streaming-Verfahrens nicht erforderlich und bildet daher keinen wesentlichen Teil eines technischen Verfahrens. Somit scheitert die Anwendung der Schranke zugunsten von vorübergehenden Vervielfältigungen nach Art. 24a URG auch an diesem Punkt.

**C. Ausschliesslich der Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder einer rechtmässigen Nutzung dienende Vervielfältigung (lit. c)**

Gemäss Art. 24a lit. c URG muss die Vervielfältigung zumindest alternativ 181 entweder ausschliesslich der Übertragung in einem Netz zwischen Dritten durch einen Vermittler (a) oder einer rechtmässigen Nutzung (b) dienen.

**a) Privilegierung von Internetzugangsanbietern**

Die erste Tatbestandsvariante privilegiert nach h.M. einzig den Vermittler 182 (i.d.R. ein *Access-Provider*), dessen Funktion sich auf die Datenübertragung für fremde Zwecke beschränkt.<sup>421</sup> Erfasst werden bspw. Speicherungen, die auf den *Servern* der *Access-Provider* entstehen, wenn jemand Werke oder andere Schutzgegenstände über das Internet abrufen, wobei es auf die Rechtmässigkeit der Nutzung durch den Endnutzer nicht ankommt.<sup>422</sup>

**b) Rechtmässige Nutzung**

**aa) Einwilligung des Rechteinhabers**

Mit der Einwilligung zur Verwertung eines Werks mittels *Streaming-Verfahren* 183 erteilt der Urheber zugleich auch seine Zustimmung betreffend die technisch bedingten, flüchtigen Teilervielfältigungen, die bei der Werkwiedergabe auf

---

<sup>420</sup> GALETZKA/STAMER, MMR 2014, 296; HILGERT/HILGERT, MMR 2014, 86; STIEPER, MMR 2012, 15; BUSCH, GRUR 2011, 501.

<sup>421</sup> OERTLI, SHK URG, Art. 24a N 9 f.; JOLLER, 148 f.; FRECH, 298; BARRELET/EGLOFF, Art. 24a N 6; REHBINDER/VIGANÒ, Art. 24a N 7; CHERPILLOD, Jusletter vom 11. Februar 2008, Rz. 22.

<sup>422</sup> OERTLI, SHK URG, Art. 24a N 10; REHBINDER/VIGANÒ, Art. 24a N 7; Botschaft URG 2006, 3430.

den Endgeräten der Rezipienten angefertigt werden.<sup>423</sup> Bei vorübergehenden Vervielfältigungen, die beim Abruf lizenzierter Streaming-Angebote hergestellt werden, ist das Kriterium der rechtmässigen Nutzung erfüllt.<sup>424</sup>

*bb) Vervielfältigung wird durch eine andere Schranke für erlaubt erklärt*

- 184 Gewisse Autoren betrachten das Tatbestandsmerkmal der rechtmässigen Nutzung auch bei nicht-lizenzierten Angeboten als erfüllt, vorausgesetzt, dass die Werknutzung durch eine (andere) Schrankenregelung des Urheberrechts gedeckt ist.<sup>425</sup>
- 185 Diese Auslegung ist problematisch, weil die in Art. 24a URG statuierte Schrankenregelung weitgehend inhaltsleer und überflüssig würde, da ihr ein eigenständiger Anwendungsbereich fehlen würde.<sup>426</sup> Eine solche inhaltsleere Regelung kann aber nicht gewollt sein.<sup>427</sup> Zudem lässt der Lösungsansatz unberücksichtigt, dass vorübergehende Vervielfältigungen, die beim Streaming nicht-lizenzierter Angebote im Rahmen der beruflichen Werknutzung hergestellt werden, strafbar wären, sofern keine Einwilligung der Rechteinhaber vorliegt, da Art. 19 Abs. 1 lit. a URG nur die Verwendung für den Privatgebrauch zulässt.<sup>428</sup> Der Nutzer wird regelmässig – wenn überhaupt – erst nach dem erfolgten Abruf eines Streams oder einer Website in der Lage sein zu beurteilen, ob es sich dabei um nicht-lizenzierte geschützte Werke handelt. Zu diesem Zeitpunkt hat die urheberrechtswidrige Vervielfältigung aber bereits stattgefunden.<sup>429</sup> Dies widerspricht der Intention des Gesetzgebers, welcher mit der Schaffung dieser Bestimmung den „Erfordernissen der modernen

---

<sup>423</sup> BRÄNDLI/TAMÖ, sic! 2013, 658; BARRELET/EGLOFF, Art. 24a N 6; zum deutschen Recht METZGER, GRUR 2012, 124.

<sup>424</sup> BRÄNDLI/TAMÖ, sic! 2013, 658; LAUBER/SCHWIPPS, GRUR 2004, 295.

<sup>425</sup> BRÄNDLI/TAMÖ, sic! 2013, 658; OERTLI, SHK URG, Art. 24a N 11; BARRELET/EGLOFF, Art. 24a N 6; vgl. zum deutschen Recht SCHÄUFELE, 102; RADMANN, ZUM 2010, 391.

<sup>426</sup> Vgl. HILGERT/GRETH, 110; MAY, 180; STOLZ, MMR 2013, 356 m.w.H.; BUSCH, GRUR 2011, 502; FANGEROW/SCHULZ, GRUR 2010, 681; LAUBER/SCHWIPPS, GRUR 2004, 295.

<sup>427</sup> BORNHAUSER, Rz. 376; vgl. zum deutschen Recht ENSTHALER, NJW 2014, 1555; STOLZ, MMR 2013, 356; BUSCH, GRUR 2011, 502; FANGEROW/SCHULZ, GRUR 2010, 681; LAUBER/SCHWIPPS, GRUR 2004, 295.

<sup>428</sup> Zur Rechtslage in Deutschland vgl. STOLZ, MMR 2013, 356; BUSCH, GRUR 2011, 501.

<sup>429</sup> MAY, 192, weist darauf hin, dass „in diesen Konstellationen die subjektive Tatbestandsseite mangels Vorsatz nicht erfüllt wäre“; BUSCH, GRUR 2011, 502.



Kommunikationstechnologie<sup>430</sup> Rechnung tragen wollte. Folglich muss die rechtmässige Nutzung i.S.v. Art. 24a URG einen über den Anwendungsbereich von Art. 19 Abs. 1 lit. a URG hinausgehenden Gehalt haben.<sup>431</sup>

cc) *Rechtmässigkeit der Quelle*

Die Vertreter der Rechteinhaber kritisieren, dass die Schweizer Nutzer durch die Legalisierung des Downloads aus illegaler Quelle ermuntert würden, gegenüber illegalen Angeboten eine pauschal unkritische Haltung einzunehmen und den Bezug von Musik und Filmen aus solchen „Gratisangeboten“ für selbstverständlich ansehen. Daraus würden (finanzielle) Schäden für die Künstler und Produzenten resultieren sowie nachhaltig die Entwicklung, der Ausbau und der Erfolg von legalen und innovativen Geschäftsmodellen behindert.<sup>432</sup>

Der Bundesrat begründete den Verzicht auf eine Einschränkung des Privatgebrauchs auf die Nutzung legaler Angebote mit der Schwierigkeit, zwischen legalen und illegalen Quellen unterscheiden zu können.<sup>433</sup> Eine Pönalisierung von Werkvervielfältigungen aus rechtswidriger Quelle wäre ein Paradigmenwechsel im Schweizer Urheberrecht. Im Gegensatz zum deutschen Urheberrecht, welches die Herstellung von Werkvervielfältigungen zum Privatgebrauch nur dann erlaubt, wenn nicht eine offensichtlich rechtswidrig hergestellte oder zugänglich gemachte Vorlage verwendet wird, kennt das schweizerische Urheberrecht keine solche Einschränkungen bei Werkverwendungen innerhalb des Privatgebrauchs.<sup>434</sup> Art. 19 Abs. 1 URG müsste *de lege ferenda* um einen Vorbehalt ergänzt werden, dass zur Vervielfälti-

<sup>430</sup> Botschaft URG 2006, 3402, 3430.

<sup>431</sup> Vgl. zum deutschen Recht GALETZKA/STAMER, MMR 2014, 296; STOLZ, MMR 2013, 356, m.w.H.; BUSCH, GRUR 2011, 502; FANGEROW/SCHULZ, GRUR 2010, 681; LAUBER/SCHWIPPS, GRUR 2004, 295; a.A. EICHELBERGER, 40 f.

<sup>432</sup> Vgl. dazu AGUR12, Schlussbericht, 51.

<sup>433</sup> Botschaft URG 2006, 3429 f.; vgl. zur (abweichenden) Rechtslage in Deutschland HILGERT/GRETH, 110 f.; HILGERT/HILGERT, MMR 2014, 85.

<sup>434</sup> Vgl. Rz. 203; zum deutschen Recht vgl. § 53 Abs. 1 UrhG, wonach einzelne Vervielfältigungen eines Werkes durch eine natürliche Person zum privaten Gebrauch auf beliebigen Trägern zulässig sind, sofern sie weder unmittelbar noch mittelbar Erwerbszwecken dienen und soweit „zur Vervielfältigung [nicht] eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird“; REDLICH, K&R 2014, 75 f.; BUSCH, GRUR 2011, 502; kritisch dazu ENSTHALER, NJW 2014, 1556, dar darauf verweist, dass § 44a Nr. 2 UrhG nicht an die Rechtmässigkeit der Vorlage anknüpft, sondern auf die Rechtmässigkeit der Nutzung selbst abstellt.

gung keine (offensichtlich) rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet werden darf.<sup>435</sup> Auch der Wortlaut des Tatbestandsmerkmals von Art. 24a lit. c URG, der von einer „rechtmässigen Nutzung“ spricht, müsste dahin gehend angepasst werden, dass nur solche Vervielfältigungen von der Schranke erfasst werden, bei denen die Kopiervorlagen nicht (offensichtlich) rechtswidrig hergestellt oder zugänglich gemacht worden sind.

- 188 Die Pönalisierung von Downloads aus illegaler Quelle steht derzeit nicht zur Debatte. Die AGUR12 hält in ihrem Schlussbericht vom 28. November 2013 sogar ausdrücklich fest, dass der Download aus illegaler Quelle zulässig bleiben soll.<sup>436</sup> In seiner Pressemitteilung vom 6. Juni 2014 liess der Bundesrat diese Einschätzung der AGUR12 unwidersprochen, obwohl der EuGH in der Zwischenzeit entschieden hatte, dass eine Schranke zum Privatgebrauch, welche nicht danach differenziert, ob die freigestellte Vervielfältigung ab rechtmässiger oder unrechtmässiger Quelle hergestellt wurde, mit dem Unionsrecht unvereinbar sei.<sup>437</sup>
- 189 Mit Blick auf die Rechtslage *de lege lata* kann festgehalten werden, dass eine Anknüpfung an die Rechtmässigkeit der Quelle weder vom Wortlaut von Art. 24a lit. c URG gedeckt wird, noch liesse sich eine solche Einschränkung mit der Schranke zum Privatgebrauch nach Art. 19 Abs. 1 lit. a URG in Einklang bringen. Letztgenannte Bestimmung erlaubt im engen Rahmen des Privatgebrauchs sogar ausdrücklich die Herstellung dauerhafter Kopien, ohne dabei zu unterscheiden, ob die Kopiervorlage aus legaler oder illegaler Quelle stammt.<sup>438</sup> Deshalb müssen dem *argumentum a maiore ad minus* folgend innerhalb des Privatgebrauchs auch vorübergehende Vervielfältigungen aus unrechtmässiger Quelle zulässig sein. Eine Pönalisierung der Nutzer durch Anknüpfung an die Rechtmässigkeit der Quelle würde zudem eine ungerechtfertigte Ausweitung der Strafbarkeit auf die Nutzer bedeuten.<sup>439</sup> Letztlich sind es die Anbieter, die durch das Verbreiten nicht-

---

<sup>435</sup> Vgl. dazu auch den Vorbehalt im deutschen Recht in § 53 Abs. 1 UrhG, wonach Vervielfältigungen dann nicht zulässig sind, wenn eine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird; EICHELBERGER, 36 ff., mit Kriterien zur Beurteilung der Offensichtlichkeit der Rechtswidrigkeit.

<sup>436</sup> AGUR12, Schlussbericht, 73.

<sup>437</sup> EuGH vom 10. April 2014, Rechtssache C-435/12, ACI Adams B.V. et al./Stichting de ThuisKopie et al.; WIGGER, UFITA II/2014, 519 f.; WIGGER, sic! 2014, 655.

<sup>438</sup> S.u. Rz. 203.

<sup>439</sup> Vgl. dazu auch VIANELLO, CR 2010, 730.

lizenzierter Werke eine Urheberrechtsverletzung begehen und nicht die Nutzer, welche diese abrufen.<sup>440</sup> Aus diesen Gründen ist eine Anknüpfung an die Rechtmässigkeit der Quelle als Tatbestandserfordernis für eine *rechtmässige Nutzung* i.S.v. Art. 24a lit. c URG abzulehnen.

dd) *Rechtmässigkeit der Nutzungshandlung*

Andere Autoren weisen darauf hin, dass die technisch bedingten Zwischenspeicherungen beim Konsum digitaler Werke letztlich dem Werkgenuss dienen.<sup>441</sup> Die Gefahr einer zweckwidrigen Verwendung von Zwischenspeicherungen ist der Nutzung von Werken in digitaler Form inhärent. In der blossen (technischen) Möglichkeit, dass vorübergehende Vervielfältigungen in einer nicht ausschliesslich dem Werkgenuss dienenden Weise verwendet werden können, sei aber noch kein über die rechtmässige Nutzung hinausgehender Vorteil zu sehen.<sup>442</sup> Ein Abstellen auf die technischen Besonderheiten der unterschiedlichen Speichervorgänge bei der Wiedergabe von digitalen Werken mittels Streaming führt zu erheblichen Rechtsunsicherheiten. Der Durchschnittsnutzer kann diese automatischen Speichervorgänge i.d.R. weder beeinflussen noch wird er diese i.d.R. überhaupt bemerken.<sup>443</sup> EICHELBERGER differenziert zwischen der auf der Tatbestandsseite vorausgesetzten Nutzungshandlung und den dazu (technisch) notwendigen Vervielfältigungshandlungen.<sup>444</sup> Entscheidend für die Rechtmässigkeit soll dabei nur die Werknutzung sein, zu deren Ermöglichung die zu rechtfertigenden technisch bedingten Vervielfältigungen hergestellt werden.<sup>445</sup> Die relevante Nutzungshandlung beschränkt

<sup>440</sup> Zur Rechtslage in Deutschland ENSTHALER, NJW 2014, 1556 f., der eine Haftung der Endnutzer – aus quasi wirtschaftlichen Gründen – als rechtlich nicht begründbar ablehnt; MAY, 182; STOLZ, MMR 2013, 357 f.

<sup>441</sup> ZECH, ZUM 2014, 6; STOLZ, MMR 2013, 357, spricht davon, dass die Vervielfältigung gleichsam eine Art Annex der Rezeption sei, die aus der besonderen Form der Wiedergabe resultiert; BORNHAUSER, Rz. 377, wendet ein, dass dem Tatbestandserfordernis der rechtmässigen Nutzung nur dann eine gewisse Bedeutung zukommt, „wenn man – entgegen dem Wortlaut, jedoch dem *argumentum a maiore ad minus* folgend – unter „Nutzung“ auch den *Werkgenuss* subsumiert und zudem vom Grundsatz der Rezeptionsfreiheit ausgeht [...]“. Da der Werkgenuss bei Anerkennung des Grundsatzes der Rezeptionsfreiheit *per se* rechtmässig ist, müssen auch die für den Werkgenuss im digitalen Bereich erforderlichen Vervielfältigungen rechtmässig sein; STIEPER, MMR 2012, 15 f.; FANGEROW/SCHULZ, GRUR 2010, 680 f.

<sup>442</sup> STIEPER, MMR 2012, 16; BORNHAUSER, Rz. 383.

<sup>443</sup> BUSCH, GRUR 2011, 502; LONGOLIUS, 47 ff.

<sup>444</sup> EICHELBERGER, 42.

<sup>445</sup> EICHELBERGER, 42; VON DIEMAR, 37 f.

sich gewöhnlich auf den Konsum des mittels Streaming übertragenen Werks.<sup>446</sup> Aufgrund des urheberrechtlichen Grundsatzes der Rezeptionsfreiheit würde sich die Frage nach der Rechtmässigkeit des Werkgenusses gar nicht stellen, da dieser *per se* rechtmässig ist und zwar unabhängig davon, ob der konsumierte Inhalt rechtmässig zugänglich gemacht bzw. verbreitet wurde.<sup>447</sup> Ein Verbot von technisch bedingten Zwischenspeicherungen, die beim Konsum digitaler Werke hergestellt werden, würde im Endeffekt einem Verbot des Werkgenusses gleichkommen.<sup>448</sup>

- 191 Damit eine sinnvolle Nutzung digitaler Werke sowohl im privaten als auch im beruflichen Bereich möglich ist, sollte das Tatbestandsmerkmal der „rechtmässigen Nutzung“ in Art. 24a lit. c URG sämtliche vorübergehenden Vervielfältigungen erfassen, die zur Wiedergabe des digitalen Werks technisch notwendig sind.<sup>449</sup>

#### **D. Die Vervielfältigung hat keine eigenständige wirtschaftliche Bedeutung (lit. d)**

- 192 In der Lehre werden verschiedene Meinungen vertreten, wann das Vorliegen einer eigenständigen wirtschaftlichen Bedeutung zu bejahen sei.<sup>450</sup> Nachfol-

---

<sup>446</sup> EICHELBERGER, 43.

<sup>447</sup> BORNHAUSER, Rz. 378. Vgl. zum deutschen Recht REDLICH, K&R 2014, 76; STOLZ, MMR 2013, 357 f.; a.A. LAUBER/SCHWIPPS, GRUR 2004, 296, die nur die Benutzung eines zuvor auf rechtmässige Weise erlangten Vervielfältigungsstücks für zulässig erachten.

<sup>448</sup> SCHEDER-BIESCHIN, 170; STOLZ, MMR 2013, 357, mit Verweis auf den urheberrechtlichen Grundsatz der Rezeptionsfreiheit; EICHELBERGER, 42, der darauf verweist, dass der blosser Werkgenuss urheberrechtlich irrelevant ist.

<sup>449</sup> Diese weite Auslegung wird auch vom Willen des Gesetzgebers gedeckt, welcher mit Einführung dieser Bestimmung den Erfordernissen der modernen Kommunikationstechnologie Rechnung tragen wollte, indem bestimmte, technisch bedingte Vervielfältigungen vom Schutzbereich des Urheberrechts ausgenommen werden, Botschaft URG 2006, 3430; vgl. auch HÜRLIMANN, 44, der darauf hinweist, dass „ein Ausschliesslichkeitsrecht in Bezug auf das nutzerseitige Browsing dem Urheber keinerlei Vorteile bringt“.

<sup>450</sup> BERANEK ZANON/DE LA CRUZ BÖHRINGER, sic! 2013, 673; BRÄNDLI/TAMÒ, sic! 2013, 658; OERTLI, SHK URG, Art. 24a N 12; BORNHAUSER, Rz. 385 ff.; BARRELET/EGLOFF, Art. 24a N 7; REHBINDER/VIGANÒ, Art. 24a N 9; BÜHLER, 166; Vgl. zum deutschen Recht STOLZ, MMR 2013, 356; STIEPER, MMR 2012, 16; EICHELBERGER, 43; BUSCH, GRUR 2011, 502; BOTT/CONRAD/JOACHIM/NORDEMANN/PILLA, GRUR-Int. 2011, 912; RADMANN, ZUM 2010, 390; FANGEROW/SCHULZ, GRUR 2010, 680.

gend werden die unterschiedlichen Ansichten aufgezeigt, bewertet und gegebenenfalls durch weitere Lösungsvorschläge ergänzt.

**a) Möglichkeit der Erzielung zusätzlicher Einnahmen**

Gewisse Autoren vertreten die Auffassung, dass eine eigenständige wirtschaftliche Bedeutung i.S.v. Art. 24a lit. d URG bereits dann anzunehmen sei, wenn den Rechteinhabern durch die Vervielfältigung die Möglichkeit der Erzielung zusätzlicher Einnahmen (etwa von Lizenzeinnahmen) entgeht.<sup>451</sup> Da beim Streaming von nicht-lizenzierten Werken kein Entgelt an die Rechtsinhaber zurückfließt, müsse das Vorliegen einer eigenständigen wirtschaftlichen Bedeutung bejaht werden.<sup>452</sup> 193

Problematisch an dieser Auslegung ist der Umstand, dass im Grundsatz für sämtliche urheberrechtlich geschützten Werke ein Markt besteht, auf dem Einnahmen durch deren Verwertung erzielt werden könnten (z.B. durch das Schalten von Werbeanzeigen).<sup>453</sup> Dies führt dazu, dass die Nutzer dafür haften müssen, wenn die Anbieter ihrer Pflicht zur Einholung der benötigten Lizenzen nicht nachgekommen sind. Die Nutzer werden zumeist nicht beurteilen können, ob der Anbieter für sämtliche Werke die benötigten Lizenzen eingeholt hat. Folglich wären sie bei der Internetnutzung konstant der Gefahr ausgesetzt, eine Urheberrechtsverletzung zu begehen. Erschwerend kommt hinzu, dass die Nutzer – wenn überhaupt – erst nach erfolgtem Abruf in der Lage sind zu beurteilen, ob die gestreamte Datei urheberrechtlich geschützte Inhalte enthält. Zu diesem Zeitpunkt hat die Vervielfältigung aber bereits stattgefunden.<sup>454</sup> Diese Auffassung ist deshalb – obschon grundsätzlich vom weitgefassten Wortlaut von Art. 24a lit. d URG gedeckt – abzulehnen.<sup>455</sup> 194

<sup>451</sup> BRÄNDLI/TAMÒ, sic! 2013, 658; weiter sind solche Tendenzen auch in der deutschen Rechtsprechung zu beobachten, vgl. BGH, Az. I ZR 69/08, GRUR 2010, 630; OLG Jena, Az. 2 U 319/07, GRUR-RR 2008, 224 f.; LG München, Az. 7 O 7061/06, MMR 2007, 329.

<sup>452</sup> BRÄNDLI/TAMÒ, sic! 2013, 658; a.A. STOLZ, MMR 2013, 356 und BUSCH, GRUR 2011, 501.

<sup>453</sup> STOLZ, MMR 2013, 356; BUSCH, GRUR 2011, 501.

<sup>454</sup> BUSCH, GRUR 2011, 502.

<sup>455</sup> Vgl. EICHELBERGER, 43.

**b) *Möglichkeit einer quantitativ oder qualitativ anderen Nutzung***

- 195 Gewisse Autoren wollen eine eigenständige wirtschaftliche Bedeutung dann bejahen, wenn durch die vorübergehende Vervielfältigung eine *quantitativ oder qualitativ andere Nutzung* der Inhalte ermöglicht wird.<sup>456</sup> Da Zwischenspeicherungen, wie sie etwa beim *Caching* oder *Browsing* anfallen, aber gerade eine intensivere und damit qualitativ bessere Nutzung ermöglichen und diese Vorgänge gemäss Botschaft erlaubt werden sollen, ist das Abgrenzungskriterium der *Möglichkeit einer quantitativ oder qualitativ anderen Nutzung* ungeeignet.<sup>457</sup> Obschon die Zwischenspeicherungen beim sog. *http-Pseudo-Streaming* ein verzögerungsfreies Vor- und Zurückspulen innerhalb der Mediendatei ermöglichen, führt dies nicht zu einer eigenständigen wirtschaftlichen Bedeutung, weil diese Speichervorgänge bloss integraler Teil des technischen

---

<sup>456</sup> OERTLI, SHK URG, Art. 24a N 12; WEBER, E-Commerce, 268 f.; BARRELET/EGLOFF, Art. 24a N 7; REHBINDER/VIGANÒ, Art. 24a N 9, sehen das Kriterium der eigenständigen wirtschaftlichen Bedeutung als erfüllt an, wenn die Vervielfältigung – auch nur mittelbar – neue, eigenständige Nutzungsmöglichkeiten eröffnet; HÄUPTLI, 147; zur Rechtslage in Deutschland BOTT/CONRAD/JOACHIM/NORDEMAN/PILLA, GRUR-Int. 2011, 912; RADMANN, ZUM 2010, 390; FANGEROW/SCHULZ, GRUR 2010, 680.

<sup>457</sup> Vgl. dazu BORNHAUSER, Rz. 105 ff. und 385, wonach die vorübergehenden Vervielfältigungen im *Cache-Speicher* beim Streaming ab einem *Webserver* gerade deshalb angefertigt werden, um eine effizientere Nutzung zu ermöglichen; Botschaft URG 2006, 3431. Vgl. zum deutschen Recht BRUNOTTE, 90 ff.; MAY, 183; REDLICH, K&R 2014, 76, der eine eigenständige wirtschaftliche Bedeutung verneint, wenn sich der wirtschaftliche Wert der Zwischenspeicherung in der Wiedergabe der Inhalte erschöpft. „Soweit über den Wiedergabevorgang hinaus keine längerfristige Speicherung der aufgerufenen Mediendatei erfolgt, die einen Werkgenuss unabhängig von der Quelle ermöglicht, fehlt es daher an einer eigenständigen wirtschaftlichen Bedeutung“; HILGERT/HILGERT, MMR 2014, 87 f.; MÜLLER, ZUM 2014, 17; STOLZ, MMR 2013, 356, mit dem Hinweis, dass es widersinnig wäre, dem temporären Speichern einer Mediendatei im Rahmen des Streamings eine eigenständige wirtschaftliche Bedeutung beizumessen, während vorübergehende Vervielfältigungen im Rahmen des Browsing und Caching nicht von eigenständiger wirtschaftlicher Bedeutung sein sollen; WANDTKE/VON GERLACH, GRUR 2013, 682 f., der die Zwischenspeicherung im *Cache-Speicher* dem Bereich des „indirekten rezeptiven Werkgenusses“ zuordnet und dieser deshalb eine eigenständige wirtschaftliche Bedeutung abspricht; STIEPER, MMR 2012, 16, nach dessen Ansicht eine eigenständige wirtschaftliche Bedeutung erst dann anzunehmen ist, „wenn die Speicherung auch nach Beendigung des jeweiligen Abspielvorgangs eine erneute Wiedergabe der Inhalte aus dem Puffer ermöglicht, ohne dass der Stream neu gestartet werden muss“; a.A. BOTT/CONRAD/JOACHIM/NORDEMAN/PILLA, GRUR-Int. 2011, 912; RADMANN, ZUM 2010, 390.

Wiedergabevorganges sind und dessen Funktionalität gewährleisten.<sup>458</sup> Letztlich besteht bei der Zwischenspeicherung digitaler Daten stets die Möglichkeit – etwa durch Manipulation des technischen Verfahrens bei der Werkwiedergabe – dauerhafte Vervielfältigungen herzustellen, weshalb dieser Lösungsansatz abzulehnen ist.<sup>459</sup>

**c) *Über die rechtmässige Nutzung hinausgehender wirtschaftlicher Nutzen aus Sicht des Rezipienten***

Weiter wird die Ansicht vertreten, dass das Vorliegen einer *eigenständigen wirtschaftlichen Bedeutung* dann zu bejahen sei, wenn aus Sicht des Rezipienten der wirtschaftliche Nutzen der Vervielfältigung, die mit der Werkwiedergabe als rechtmässige Nutzung ohnehin verbundenen Vorteile übersteigt.<sup>460</sup> In die gleiche Richtung zielt auch die Meinung von BORNHAUSER, wonach die *eigenständige wirtschaftliche Bedeutung* bei flüchtigen Vervielfältigungen erst dann anzunehmen sei, wenn aufgrund des konkreten (technischen) Umfelds davon ausgegangen werden muss, dass die Werkvervielfältigungen in einer von Art. 5 Abs. 1 lit. a oder b Info-Richtlinie abweichenden Weise verwendet werden.<sup>461</sup> Letztlich bleibt aber auch bei diesem Lösungsansatz unklar, welche Abgrenzungskriterien für die „Annahme einer Verwendung in abweichender Weise“ herangezogen werden sollen.

STIEPER plädiert dafür, dass eine *eigenständige wirtschaftliche Bedeutung* erst dann angenommen werden sollte, wenn die gestreamten Inhalte sukzessive und dauerhaft abgespeichert werden und vom Nutzer auch nach Beendigung der Client-Software bzw. nach Herunterfahren des Nutzerrechners verwendet werden können.<sup>462</sup> Da eine solche Vervielfältigung aber weder flüchtig oder begleitend (lit. a) noch ein integraler oder wesentlicher Teil eines technischen

<sup>458</sup> HILGERT/GRETH, 112; REDLICH, K&R 2014, 76; GALETZKA/STAMER, MMR 2014, 293; STIEPER, MMR 2012, 16; LONGOLIUS, 44 ff.

<sup>459</sup> HILGERT/GRETH, 111 f.; HILGERT/HILGERT, MMR 2014, 87; STIEPER, MMR 2012, 16.

<sup>460</sup> GALETZKA/STAMER, MMR 2014, 297; STOLZ, MMR 2013, 356; STIEPER, MMR 2012, 16; EICHELBERGER, 43; VON GERLACH, 189; BUSCH, GRUR 2011, 502.

<sup>461</sup> BORNHAUSER, Rz. 369 und 386; Art. 5 Abs. 1 lit. a und b der Info-Richtlinie decken sich inhaltlich mit Art. 24a lit. a-c URG.

<sup>462</sup> STIEPER, MMR 2012, 16, plädiert dafür, eine eigenständige wirtschaftliche Bedeutung erst dann anzunehmen, „wenn die Speicherung auch nach Beendigung des jeweiligen Abspielvorgangs eine erneute Wiedergabe der Inhalte aus dem Puffer ermöglicht, ohne dass der Stream neu gestartet werden muss“. Sogleich folgt eine Einschränkung, dass die Schranke auch dann greifen soll, wenn die Zwischenspeicherungen spätestens beim Beenden der Client-Software automatisch gelöscht werden; ebenso EICHELBERGER, 43.

Verfahrens ist (lit. b), kommt die Schranke für vorübergehende Vervielfältigungen ohne eigenständige wirtschaftliche Bedeutung nach Art. 24a URG ohnehin nicht zur Anwendung.<sup>463</sup>

**d) *Ersatzlose Streichung des negativen Tatbestandserfordernisses der fehlenden eigenständigen wirtschaftlichen Bedeutung***

- 198 Mit Blick auf die verschiedenen Lehrmeinungen zeigt sich eine allgemeine Verwirrung betreffend die Auslegung des Kriteriums der fehlenden eigenständigen wirtschaftlichen Bedeutung. Es fehlen klare Abgrenzungskriterien, was unweigerlich zu Rechtsunsicherheit führt. Sogar ein technisch versierter Nutzer wird häufig nicht in der Lage sein zu beurteilen, in welchem Umfang ein Werk während der Streaming-Wiedergabe auf seinem Rechner zwischengespeichert wird.<sup>464</sup> Werden die Inhalte bei der Wiedergabe des Streams dauerhaft auf einem Speichermedium im Nutzerrechner abgespeichert, scheitert die Berufung auf die Schranke zugunsten vorübergehender Vervielfältigungen bereits deshalb, weil die Vervielfältigung nicht bloss flüchtig oder begleitend ist (Art. 24a lit. a URG). Der *eigenständigen wirtschaftlichen Bedeutung* kommt folglich keine über die Tatbestandsvoraussetzungen von Art. 24a lit. a-c URG hinausgehende Beschränkungsfunktion zu.<sup>465</sup> Solange die Voraussetzungen von Art. 24a lit. a-c URG erfüllt sind, ist auch das negative Tatbestandserfordernis der fehlenden *eigenständigen wirtschaftlichen Bedeutung* nach Art. 24a lit. d URG zu bejahen. *De lege ferenda* könnte deshalb über eine ersatzlose Streichung des Tatbestandsmerkmals der fehlenden wirtschaftlichen Bedeutung nachgedacht werden, da dieses mehr Verwirrung stiftet als Klarheit schafft.

---

<sup>463</sup> Vgl. EICHELBERGER, 43.

<sup>464</sup> WANDTKE/VON GERLACH, GRUR 2013, 683; BUSCH, GRUR 2011, 502; LONGOLIUS, 47 ff.

<sup>465</sup> Ebenso BORNHAUSER, Rz. 388, m.w.H.; vgl. zum deutschen Recht MARLY, EuZW 2014, 619 und ENSTHALER, NJW 2014, 1555, die darauf hinweisen, dass die Merkmale der rechtmässigen Nutzung und der eigenständigen wirtschaftlichen Bedeutung nur schwer voneinander getrennt betrachtet werden können.



## 2. Schranke des Privatgebrauchs (Art. 19 Abs. 1 lit. a URG)

Art. 19 Abs. 1 lit. a URG verleiht dem Nutzer eine Befugnis, wonach im persönlichen Bereich und innerhalb eines privaten Kreises von ihm nahestehenden Personen (z.B. enge Freunde und Verwandte) jede Werkverwendung zulässig ist.<sup>466</sup> In dieser Lizenz miteingeschlossen ist nicht nur das Vervielfältigungsrecht zu privaten Zwecken, sondern jegliche Werkverwendung im privaten Kreis.<sup>467</sup> Demgegenüber kann nicht mehr von Privatgebrauch im Sinne dieses Gesetzes gesprochen werden, wenn beliebige Dritte Zugriff auf das Werk erhalten.<sup>468</sup> Weiter wird in jedem Fall vorausgesetzt, dass das Werk bereits veröffentlicht wurde.<sup>469</sup> Der private Nutzer darf auch einen Dritten zur Herstellung einer Privatkopie heranziehen.<sup>470</sup> Mit der Schrankenregelung zum Privatgebrauch soll einerseits die Privatsphäre vor dem Zugriff der Rechtsverfolgung gewahrt bleiben und andererseits die unkontrollierbare Massennutzung nicht für illegal gelten, ohne dass entsprechende Urheberrechtsverletzungen auch tatsächlich rechtswirksam verfolgt und geahndet werden können.<sup>471</sup>

Art. 19 Abs. 4 URG statuiert eine wichtige Ausnahme, wonach die Schrankenregelung von Art. 19 URG keine Anwendung auf Computerprogramme finden soll.<sup>472</sup> Massgebend für die Verwendung von Computerprogrammen sind insbesondere die Sondervorschriften zum bestimmungsgemässen Ge-

<sup>466</sup> GASSER, SHK URG, Art. 19 N 6 ff.; BARRELET/EGLOFF, Art. 19 N 8; REHBINDER/VIGANÒ, Art. 19 N 11 f.; BAUMGARTNER, 83 f.; GLARNER, sic! 2006, 641.

<sup>467</sup> CHERPILLOD, SIWR II/1, 264; BRÄNDLI/STRASZ, 89; BARRELET/EGLOFF, Art. 19 N 8; DESSEMONTET, droit d'auteur, 314; BÜHLER, 255; GASSER, 50 ff., mit Hinweis auf die zum Privatgebrauch berechtigten Personenkreise.

<sup>468</sup> GASSER, SHK URG, Art. 19 N 7; BARRELET/EGLOFF, Art. 19 N 8; REHBINDER/VIGANÒ, Art. 19 N 16; BÜHLER, 256.

<sup>469</sup> BRÄNDLI/STRASZ, 89; HILTY, Urheberrecht, Rz. 220.

<sup>470</sup> BGE 140 III 616, Erw. 3.4.2; BIELER, sic! 2015, 163 ff.; BRÄNDLI/STRASZ, 90; GASSER, SHK URG, Art. 19 N 13 und N 24 ff., spricht beim Beizug eines Dritten von einem „Privatgebrauch im weiten Sinne“; REHBINDER/VIGANÒ, Art. 19 N 17; BÜHLER, 261; GASSER, 37, mit dem Hinweis, dass es dem Dritten untersagt ist, Vervielfältigungen auf Vorrat hin anzufertigen oder eine Tätigkeit auszuüben, die jener eines Verlags gleichkommt.

<sup>471</sup> REHBINDER/VIGANÒ, Art. 19 N 12; GIRSBERGER, 2; AUF DER MAUR/KELLER, sic! 2004, 79; GASSER, 17 ff.; Botschaft URG 1989, 538.

<sup>472</sup> GASSER, SHK URG, Art. 19 N 49; REHBINDER/VIGANÒ, Art. 19 N 38; EGLOFF, sic! 2007, 708.

brauch (Art. 12 Abs. 2 URG i.V.m. Art. 17 Abs. 1 URV), zur Entschlüsselung (Art. 21 URG i.V.m. Art. 17 Abs. 2 und 3 URV) und zur Sicherungskopie (Art. 24 Abs. 2 URG).<sup>473</sup>

- 201 Bei Werkverwendung im Rahmen des Privatgebrauchs, beschränkt sich der Vergütungsanspruch der Urheber auf die Leerträgervergütung nach Art. 20 Abs. 3 URG.<sup>474</sup> Von der Leerträgervergütung erfasst werden sowohl analoge wie digitale Ton-, Tonbild- und andere Datenträger, die geeignet sind, urheberrechtlich geschützte Werke aufzuzeichnen und angesichts des ihnen zugedachten Nutzungszwecks und ihrer Aufzeichnungs- und Wiedergabeeigenschaften voraussichtlich für solche Zwecke eingesetzt werden.<sup>475</sup>

### A. Vervielfältigungen aus unrechtmässiger Quelle

- 202 In der schweizerischen Lehre sind einige Autoren der Ansicht, dass die Schrankenregelung zum Privatgebrauch von Art. 19 Abs. 1 lit. a URG nur in jenen Fällen zur Anwendung gelangen soll, in denen kumulativ zur Voraussetzung des privaten Gebrauchszwecks auch ein rechtmässiger Zugang zur Kopiervorlage gegeben ist.<sup>476</sup> Es wird u.a. damit argumentiert, dass eine gesetzliche Erlaubnis für wissentlich und willentlich erstellte Raubkopien oder für über illegale Tauschbörsen beschaffte Werkexemplare weder mit der Eigentumsgarantie der Bundesverfassung (Art. 26 BV) noch mit dem konventionsrechtlichen Mindestschutz (WCT, TRIPS, RBÜ; entsprechend für die verwandten Schutzrechte: WPPT, Rom-Abkommen) vereinbar sei.<sup>477</sup>
- 203 Demgegenüber vertritt die h.L. die Ansicht, dass Vervielfältigungen im Rahmen des Privatgebrauchs auch dann hergestellt werden dürfen, wenn die Kopiervorlage aus einer illegalen Quelle stammt.<sup>478</sup> Die Pönalisierung des

---

<sup>473</sup> BÖTTCHER, 161, das Gebrauchsrecht verleiht dem Erwerber eines Computerprogramms das Recht, dieses zu nutzen, „worunter auch das Laden des Programms fällt“; GASSER, SHK URG, Art. 19 N 13; BARRELET/EGLOFF, Art. 19 N 29; BÜHLER, 262 ff.

<sup>474</sup> GASSER, SHK URG, Art. 20 N 12 ff., m.w.H. zur Leerträgervergütung; BÜHLER, 256.

<sup>475</sup> GASSER, SHK URG, Art. 20 N 12; GASSER, 165 ff.; BGE 133 II 263, Erw. 7.

<sup>476</sup> BRÄNDLI/STRASZ, 100 ff.; BARRELET/EGLOFF, Art. 19 N 7a und N 7b; BU, 70; GASSER, 60 ff.

<sup>477</sup> REHBINDER/VIGANÒ, Art. 19 N 19.

<sup>478</sup> WIGGER, sic! 2014, 658; CHERPILLOD, SIWR II/1, 266; BRÄNDLI/TAMÒ, sic! 2013, 658; THOUVENIN, ACTA, 112 f.; GASSER, SHK URG, Art. 19 N 10a ff.; HILTY, Urheberrecht, Rz. 176, 220 ff.; BARRELET/EGLOFF, Art. 19 N 7b; BAUMGARTNER, 200; GLARNER, sic! 2006, 646; GLARNER, Musikpiraterie im Internet, 81 ff.; kritisch DE WERRA, medialex 2006, 171 f.

privaten Downloads urheberrechtlich geschützter und widerrechtlich angebotener Werke sprengt sowohl den Wortlaut als auch den Sinn von Art. 19 Abs. 1 lit. a URG.<sup>479</sup> Zunächst darf nicht ausser Acht gelassen werden, dass bei einem unautorisierten Angebot die Urheberrechtsverletzung durch den Anbieter begangen wird. Überdies ist es für den Nutzer in vielen Fällen gar nicht überprüfbar, ob es sich um ein recht- oder unrechtmässiges Angebot handelt.<sup>480</sup> Schliesslich ist die Einführung des ungeschriebenen Tatbestandsmerkmals der Rechtmässigkeit der Quelle auch mit dem Legalitätsprinzip unvereinbar und daher abzulehnen.<sup>481</sup> Es ist vielmehr Sache des Gesetzgebers, die bestehenden Strafnormen des URG dahingehend zu ergänzen, dass private Daten-Piraten zur Verantwortung gezogen werden können.<sup>482</sup> In der Botschaft zum Bundesbeschluss über die Genehmigung von zwei Abkommen der Weltorganisation für geistiges Eigentum (WIPO) und zur Änderung des Urheberrechtsgesetzes vom 10. März 2006 wird festgehalten, dass zwar die Benutzung einer illegalen Quelle gemäss Art. 19 Abs. 3 lit. a URG unzulässig sei, weil sie dazu dienen würde, den Ankauf von im Handel erhältlichen Werkexemplaren zu umgehen.<sup>483</sup> Diese Einschränkung des Eigengebrauchs erstreckt sich aber nicht auf die Werkverwendung durch eine natürliche Person zu ihrem eigenen, persönlichen Gebrauch. Daher muss bei Werkverwendungen im engen Rahmen der Privatsphäre nicht zwischen legalen und illegalen Quellen unterschieden werden, was im Einzelfall auch schwierig sein dürfte.<sup>484</sup>

In der Revision des URG im Jahr 2007 sah der Gesetzgeber von einer Neu- 204  
regelung ab, mit der Erwägung, ein ausdrückliches Verbot würde den privaten Nutzern eine Rechtmässigkeitsprüfung aufbürden, die ihnen in Grenzfällen nicht zuzumuten wäre.<sup>485</sup> Zudem würden so breite Kreise kriminalisiert.<sup>486</sup> Dabei wurde jedoch verkannt, dass die Strafbarkeit bei Urheberrechtsverletzungen nach Art. 67 Abs. 1 URG stets ein vorsätzliches Handeln

<sup>479</sup> GLARNER, sic! 2006, 646; SCHWARZENEGGER, P2P-Netzwerke, 227; RIGAMONTI, GRUR-Int. 2004, 281 ff.; SCHACK, FS-Erdmann, 166.

<sup>480</sup> HAUNREITER, 108.

<sup>481</sup> Vgl. zum Ganzen GLARNER, sic! 2006, 646; SCHWARZENEGGER, P2P-Netzwerke, 227, m.w.H.

<sup>482</sup> GLARNER, sic! 2006, 646.

<sup>483</sup> Botschaft URG 2006, 3429 f.

<sup>484</sup> Vgl. Botschaft URG 2006, 3429 f.

<sup>485</sup> Amtl. Bull. NR 2007 1197.

<sup>486</sup> Vgl. Amtl. Bull. NR 2007 1202.

voraussetzt, weshalb die problematisierte Situation gar nicht erfasst wird.<sup>487</sup> Sodann hielt auch die AGUR12 in ihrem Schlussbericht vom 28. November 2013 fest, dass der Download aus illegaler Quelle zulässig bleiben soll.<sup>488</sup>

- 205 Angesichts der Tatsache, dass der Gesetzgeber auf eine Pönalisierung des Privatgebrauchs aus unrechtmässiger Quelle verzichtet hat, ist nach hier vertretener Ansicht der Meinung von GLARNER und den zitierten Ausführungen der Botschaft zu folgen<sup>489</sup>. Wenn der private Download bzw. das Streaming aus unrechtmässiger Quelle strafrechtlich sanktioniert werden sollte, müsste vom Gesetzgeber vorab eine entsprechende gesetzliche Grundlage geschaffen werden.<sup>490</sup>

## **B. Zahlenmässige Beschränkung der Privatvervielfältigungen**

- 206 Aus dem Gesetzeswortlaut ergibt sich zwar keine mengenmässige Beschränkung der privaten Vervielfältigung, jedoch lässt sich eine solche aus dem privaten Zweck ableiten, weshalb eine Anzahl Kopien, die mit dem erlaubten privaten Zweck nicht erklärbar ist, nicht mehr von der Schrankenregelung gedeckt wird.<sup>491</sup> Die beim Streaming hergestellten Vervielfältigungen auf dem Nutzerrechner dienen der Werkwiedergabe und sind deshalb ohne Weiteres mit dem privaten Zweck erklärbar.

## **C. Zulässigkeit des Streaming gestützt auf die Schrankenregelung zum Privatgebrauch**

- 207 Gestützt auf die Schrankenregelung zum Privatgebrauch nach Art. 19 Abs. 1 lit. a URG ist die Herstellung dauerhafter Werkkopien – unabhängig von der Rechtmässigkeit der Kopiervorlage – zulässig.<sup>492</sup> Folglich werden von dieser Bestimmung auch flüchtige Vervielfältigungen erfasst, sofern diese im Rahmen des Privatgebrauchs anfallen.<sup>493</sup>

---

<sup>487</sup> REHBINDER/VIGANÒ, Art. 19 N 19.

<sup>488</sup> AGUR12, Schlussbericht, 73.

<sup>489</sup> GLARNER, sic! 2006, 646; Botschaft URG 2006, 3429 f.

<sup>490</sup> GLARNER, sic! 2006, 646; AUF DER MAUER/KELLER, sic! 2004, 86 f.

<sup>491</sup> GASSER, SHK URG, Art. 19 N 9b; REHBINDER/VIGANÒ, Art. 19 N 18; zum deutschen Recht BECKER, ZUM 2012, 645 ff.

<sup>492</sup> Vgl. Rz. 203.

<sup>493</sup> Gl. M. BRÄNDLI/TAMÒ, sic! 2013, 658 f., m.w.H.

### 3. Vergütung für den Eigengebrauch (Art. 20 URG)

Gemäss Art. 20 Abs. 1 URG ist die Werkverwendung im privaten Kreis nach Art. 19 Abs. 1 lit. a URG – unter Vorbehalt von Art. 20 Abs. 3 URG – vergütungsfrei. Die Leerträgervergütung ist technologieneutral formuliert und umfasst sämtliche analogen und digitalen Datenträger, die geeignet sind, urheberrechtlich geschützte Werke abzuspeichern.<sup>494</sup> Die Leerträgervergütung umfasst auch Geräte mit fest eingebautem Speicher als Leerträger, sofern dem verbauten Speicher dieselbe oder eine vergleichbare Funktion zukommt wie den auswechselbaren Speichermedien.<sup>495</sup> Die Leerträgervergütung ist als indirektes Vergütungssystem konzipiert, da sie nicht direkt vom Eigengebrauchsberechtigten bzw. einer im Rahmen des Eigengebrauchs nach Art. 19 Abs. 2 URG handelnden Drittperson zu bezahlen ist, sondern vom inländischen Hersteller des Datenträgers bzw. vom Importeur zu entrichten ist.<sup>496</sup> Tatsächlich werden nur jene Datenträger durch die Leerträgervergütung belastet, die von den Tarifen erfasst werden.<sup>497</sup> Die Leerträgervergütung wird von den Verkäufern auf die Endkonsumenten abgewälzt, weshalb diese bereits beim Kauf eines entsprechenden Endgeräts bezahlt wird. Die Leerträgervergütung ist m.a.W. unabhängig davon geschuldet, ob der Nutzer tatsächlich urheberrechtlich relevante Werknutzungen vornimmt oder nicht. Die Ansicht, dass beim Konsum von nicht-lizenzierten Streaming-Angeboten [zum Privatgebrauch] eine Leerträgervergütung nach Art. 20 Abs. 3 URG geschuldet sei, ist abzulehnen.<sup>498</sup>

<sup>494</sup> BGE 133 II 263, Erw. 7; BERANEK ZANON/DE LA CRUZ BÖHRINGER, sic! 2013, 679; GASSER, SHK URG, Art. 20 N 12; WIGGER, sic! 2011, 196; BARRELET/EGLOFF, Art. 20 N 9; GIRSBERGER, Fn. 850; GASSER, 165 ff.

<sup>495</sup> GASSER, SHK URG, Art. 20 N 12a; GASSER, 174, 184; Von der Leerträgervergütung erfasst werden digitale Speichermedien wie Mikrochips oder Harddisks in Audio- und audiovisuellen Aufnahmegeräten durch den Gemeinsamen Tarif 4d (GT 4d), digitale Speicher in Mobiltelefonen durch den Gemeinsamen Tarif 4e (GT 4e) und digitale Speicher in Tablets durch den Gemeinsamen Tarif 4f (GT 4f), vgl. <<http://www.suisa.ch/de/kunden/tarifuebersicht>> (besucht 25. August 2015).

<sup>496</sup> BGE 133 II 263, Erw. 5.2; BERANEK ZANON/DE LA CRUZ BÖHRINGER, sic! 2013, 679, mit Hinweisen zur Leerträgervergütung beim Cloud-Computing; GASSER, SHK URG, Art. 20 N 13; BRÄNDLI/STRASZ, 92; BARRELET/EGLOFF, Art. 20 N 10; REHBINDER/VIGANÒ, Art. 20 N 3; GASSER, 148 ff., 169 ff.

<sup>497</sup> BGE 133 II 263, Erw. 7; GASSER, SHK URG, Art. 20 N 15, mit dem Hinweis, dass die Tarife aufgrund der technischen Weiterentwicklungen immer wieder aktualisiert und angepasst werden müssen.

<sup>498</sup> Wohl gl. M. BAUMGARTNER, 91; a.A. BRÄNDLI/TAMÒ, sic! 2013, 659.; JOLLER, 147; unklar BARRELET/EGLOFF, Art. 19 N 28e, sprechen von einem „sonderbaren Ergebnis, dass eine Vergütungspflicht nur für Abrufe von Werken besteht, die ohne Einwilligung

Die Leerträgervergütung knüpft nicht an das Vorliegen einer urheberrechtlich relevanten Nutzungshandlung an, sondern an analogen oder digitalen Datenträgern, welche für die Aufzeichnung geschützter Werke geeignet sind, von einem Tarif erfasst und in der Schweiz oder im Fürstentum Liechtenstein hergestellt oder importiert werden.<sup>499</sup>

- 209 Unzutreffend ist m.E. der Umkehrschluss aus Art. 19 Abs. 3<sup>bis</sup> URG, dass ein Nutzer für die beim Abruf von nicht-lizenzierten Werken hergestellten transitorischen Vervielfältigungen entschädigungspflichtig wird.<sup>500</sup> Die etwas umständliche Formulierung in Art. 19 Abs. 3<sup>bis</sup> URG sollte laut bundesrätlicher Botschaft sicherstellen, dass auf (Teil-)Vervielfältigungen von digitalen Werken, die über elektronische Bezahldienste angeboten werden, keine zusätzliche Leerträgervergütung erhoben wird.<sup>501</sup> Im Ergebnis ist daher festzuhalten, dass der Nutzer weder beim Streaming noch beim *Download* von urheberrechtlich geschützten Werken nach Art. 20 Abs. 3 URG entschädigungspflichtig wird und zwar unabhängig davon, ob es sich dabei um lizenzierte oder nicht-lizenzierte (illegale) Angebote handelt.

### III. Technische Massnahmen zum Schutz digitaler Werke beim Streaming

#### 1. Einleitung

- 210 Zum Schutz digitaler Angebote werden technische Massnahmen eingesetzt. Darunter sind sämtliche Vorrichtungen zu verstehen, die den unerlaubten Zugang zu bzw. die unerlaubte Nutzung von Werken i.S.v. Art. 2 URG kontrollieren und gegebenenfalls verhindern können.<sup>502</sup> Nachfolgend wird untersucht, welche technischen Möglichkeiten derzeit für die Rechteinhaber be-

---

der Urheberinnen und Urheber angeboten werden [...]. Wie diese Regelung umgesetzt werden soll ist unklar [...]“.

<sup>499</sup> GASSER, SHK URG, Art. 20 N 15; BARRELET/EGLOFF, Art. 20 N 10; BAUMGARTNER, 91.

<sup>500</sup> A.A. BRÄNDLI/TAMÖ, sic! 2013, 659 und wohl auch EGLOFF, medialex 2011, 78; JOLLER, 147; BARRELET/EGLOFF, Art. 19 N 28e.

<sup>501</sup> Botschaft URG 2006, 3429; BARRELET/EGLOFF, Art. 19 N 28e; BERGER, sic! 2007, 733 ff.; da die Leerträgervergütung gemäss Art. 20 Abs. 4 URG nur von zugelassenen Verwertungsgesellschaften geltend gemacht werden darf, wäre es ohnehin unzulässig, wenn die Bezahldienste hierfür ein zusätzliches Entgelt verlangen würden.

<sup>502</sup> RUBLI, Rz. 4; GIRSBERGER, 99; GLARNER, Musikpiraterie im Internet, 159.

stehen, um die Verwertung ihrer Werke mittels Streaming vor unerlaubtem Zugriff zu schützen bzw. um unerlaubte Nutzungshandlungen zu verhindern. Ebenso wird geprüft, inwieweit sich die Urheber gegen eine Umgehung der technischen Massnahmen durch die Nutzer mit rechtlichen Mitteln zur Wehr setzen können.

## 2. Technische Massnahmen

Es existiert eine Vielzahl verschiedener Technologien, welche zum Schutz 211 gegen den unerlaubten Zugriff bzw. die unerlaubte Verwendung von geschützten Werken eingesetzt werden können.<sup>503</sup> Ausgehend von der Zwecksetzung der technischen Schutzmassnahmen lassen sich diese in *zwei Kategorien* unterteilen: Die *Zugangsschranken* und die *Nutzungsschranken*.<sup>504</sup>

### A. Zugangsschranken

Als Zugangsschranken gelten jene technischen Massnahmen, die den Zu- 212 gang zu einem urheberrechtlich geschützten Werk oder zu einer durch ein verwandtes Schutzrecht geschützten Leistung bzw. Teilen davon einschränken, indem dieser von einer vorgängigen, individuellen Erlaubnis des Rechteinhabers abhängig gemacht wird.<sup>505</sup> Der Einsatz von Zugangsschranken soll gewährleisten, dass die Nutzung des Werks erst erfolgen kann, nachdem der Nutzer die Zugangsschranke passiert hat. Eine gängige Variante zum Schutz digitaler Werke besteht darin, dass der Werkzugang erst nach Eingabe einer Benutzererkennung sowie eines Passworts eingeräumt wird.<sup>506</sup> Beispiele dafür sind kostenpflichtige Video-On-Demand-Streaming-Dienste wie Netflix, Maxdome, Watchever, Amazon Prime Instant Video oder Musik-Streaming-Dienste wie Spotify oder Apple Music.

---

<sup>503</sup> GRABER, sic! 2010, 331; WAND, 7;

<sup>504</sup> RUBLI, Rz. 14; PLATZ, Jusletter vom 16. Juni 2008, Rz. 24 ff.; BERGER, SJZ 2007, 403; GIRSBERGER, 99; GLARNER, Musikpiraterie im Internet, 160; SCHACK, ZUM 2002, 504; WAND, 10; a.A. REHBINDER/VIGANÒ, Art. 39a N 12, HAUNREITER, 104 f. und GIRSBERGER, 98 f., die eine Unterteilung in Zugangs- und Nutzungsschranken aufgrund „der zunehmenden Vielfalt und Differenziertheit digitaler Verbreitungs- und Nutzungsmodelle“ ablehnen.

<sup>505</sup> RUBLI, Rz. 6 ff., spricht von Zugriffskontrollen; PLATZ, Jusletter vom 16. Juni 2008, Rz. 26 f.; REHBINDER/VIGANÒ, Art. 39a N 1; GIRSBERGER, 99; BAUMGARTNER, 18; BECHTOLD, Informationsrecht, 23 ff.; WAND, 10.

<sup>506</sup> RUBLI, Rz. 7 ff.; GLARNER, Musikpiraterie im Internet, 160.

## B. Nutzungsschranken

- 213 Durch den Einsatz von Nutzungsschranken kann der Umfang der Werknutzung (z.B. hinsichtlich der Nutzungsdauer oder der Kopierbarkeit des Werks) eingeschränkt werden.<sup>507</sup> Den in der Praxis wichtigsten Teilbereich stellen die Codier- und Kopierschutzsysteme dar.<sup>508</sup> Die Codiersysteme verhindern bzw. beschränken die Nutzung von Daten, die sich bereits in der Verfügungsmacht des Nutzers befinden, während der Kopierschutz es ermöglicht, Kopiervorgänge zu steuern oder vollständig zu unterbinden.<sup>509</sup> Eine Möglichkeit zur Verschlüsselung eines Streams bietet *RTMPE* von Adobe, mit dem sich eine verschlüsselte Verbindung zwischen *Client* und *Server* aufbauen lässt.<sup>510</sup>

## 3. DRM-Systeme (DRMS)

- 214 Die Abkürzung *DRM* steht für *Digital Rights Management*.<sup>511</sup> Darunter sind technische Massnahmen zur Verwaltung von Rechten im digitalen Umfeld zu verstehen.<sup>512</sup> Mittels *DRM* soll der automatisierte Vertrieb von Inhalten in digitaler Form ermöglicht werden.<sup>513</sup> Kennzeichnend für diese Systeme ist der Schutz der digitalen Inhalte mittels technischer Massnahmen.<sup>514</sup> Konkret wird geregelt, welche Inhalte wann, wo, wie und wie oft genutzt werden können.<sup>515</sup> Der Einsatz von *DRM* eröffnet den Rechteinhabern eine Vielzahl

---

<sup>507</sup> AUF DER MAUR, SHK URG, N 8 ff. Vorb. zu Art. 39a-c; GRABER, sic! 2010, 331 f.; HAUNREITER, 104 f.; BAUMGARTNER, 18 f.; SCHWERZMANN, sic! 2004, 150.

<sup>508</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 25; GLARNER, sic! 2006, 648.

<sup>509</sup> GLARNER, sic! 2006, 648; KNIES, ZUM 2003, 287.

<sup>510</sup> HEINEMEYER/KREITLOW, MMR 2013, 624; JANISCH/LACHENMANN, MMR 2013, 214; LONGOLIUS, 70.

<sup>511</sup> BGE 133 II 263, Erw. 10.1; BENHAMOU, 6; BÖTTCHER, 228 ff.; FITZNER, 51 ff.; SCHIPPAN, ZUM 2004, 188 ff.

<sup>512</sup> THOUVENIN, ACTA, 119; FITZNER, 51; RUNGE, GRUR-Int. 2007, 130 f.; BAUMGARTNER, 17 ff.; SCHULZ, GRUR 2006, 471; ARLT, 9; ausführlich dazu BECHTOLD, Informationsrecht, 19 ff.

<sup>513</sup> FITZNER, 51, wonach die Beschreibung, Identifikation, der Vertrieb und Schutz digitaler Werke sowie die Überwachung jeglicher in Bezug auf ein solches Werk vorgenommene Nutzerhandlung vom Begriff Digital Rights Management umfasst wird; STRAUB, 147 f.; RUBLI, Rz. 5; PFENNIG, ZUM 2004, 198 ff.; PEUKERT, sic! 2004, 749.

<sup>514</sup> RUBLI, Rz. 5; WEBER, E-Commerce, 262; SCHIPPAN, ZUM 2004, 190.

<sup>515</sup> STIEPER, MMR 2012, 13; BUSCH, GRUR 2011, 497; KOCH, GRUR 2010, 575; BORNHAUSER, Rz. 180; LONGOLIUS, 50; FETSCHERIN, Rz. 4.



von Möglichkeiten zur digitalen Individualisierung.<sup>516</sup> DRM-Systeme sind aus einer Vielzahl technischer Komponenten aufgebaut, die in ihrer Gesamtheit verschiedene Funktionen erfüllen können. So können bspw. optional Verschlüsselungs- und Kopierschutzverfahren, digitale Wasserzeichen, Metadaten sowie Rechtedefinitionssprachen eingesetzt werden.<sup>517</sup> Der digitale Inhalt befindet sich dabei in einem verschlüsselten digitalen Container, der nur durch autorisierte Nutzer unter Verwendung eines speziellen Schlüssels geöffnet werden kann. In sog. Metadaten, die sich meist unverschlüsselt auf der „Aussenhülle“ des Containers befinden, sind Informationen zum digitalen Inhalt wie bspw. Titel und Urheber des Werks sowie die Nutzungsrechte enthalten. Die Nutzungsrechte regeln etwa, ob und wie oft der digitale Inhalt kopiert oder anderen Nutzern zur Verfügung gestellt werden darf und ob die Nutzungserlaubnis auf einen bestimmten Termin hin ausläuft.<sup>518</sup>

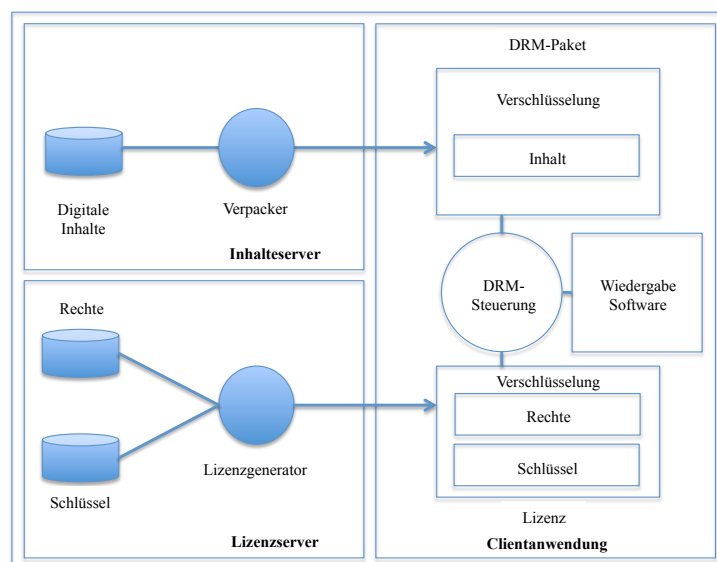


Abbildung 7: Technische Umsetzung von DRM-Systemen, Quelle: <[http://de.wikipedia.org/wiki/Digitale\\_Rechteverwaltung](http://de.wikipedia.org/wiki/Digitale_Rechteverwaltung)> (besucht 3.7.2015)

Die digitalen Inhalte werden von einem *Inhalteserver* verwaltet und mit Hilfe eines *DRM-Verpackers* zur Verwendung in einem *DRM-System* verschlü-

<sup>516</sup> FITZNER, 64 f.; HILTY, ZUM 2003, 983; kritisch RUNGE, GRUR-Int. 2007, 136 f.

<sup>517</sup> THOUVENIN, ACTA, 119; FITZNER, 53 ff.; SCHULZ, GRUR 2006, 472; SCHWERZMANN, sic! 2004, 150.

<sup>518</sup> Vgl. zum Ganzen FETSCHERIN, Rz. 4; BECHTOLD, Informationsrecht, 23 ff.

selt. Durch diesen Vorgang werden die digitalen Inhalte vorerst unlesbar gemacht. Auf Anforderung hin erzeugt ein *Lizenzserver* die erforderlichen Lizenzen zusammen mit den dazugehörigen Schlüsseln für die Benutzerauthentifizierung und Inhalteentschlüsselung, welche aus den entsprechenden Kennungen (Benutzer- oder Geräteerkennung, Inhalteerkennung) und den Beschreibungen der Rechte berechnet werden. Damit der Nutzer Zugriff auf die *DRM*-geschützten Inhalte erhält, fordert die *DRM*-Steuerung vom *Lizenzserver* die zur Wiedergabe erforderliche Lizenz an. Sobald die Authentizität und Integrität des Wiedergabeprogrammes verifiziert worden sind, werden die Inhalte durch den in der Lizenz enthaltenen Schlüssel entschlüsselt und an das Wiedergabeprogramm weitergegeben. Das Programm kann die Inhalte – da wieder lesbar – nun wiedergeben.<sup>519</sup>

- 216 Gegner von *DRM*-Systemen weisen darauf hin, dass deren Einsatz Datenschutz- oder Interoperabilitätsprobleme verursachen sowie zur Unternutzung digitaler Werke führen kann und darüber hinaus zur Förderung von Monopolstellungen einzelner Anbieter beiträgt.<sup>520</sup> Zudem wird befürchtet, dass durch den Einsatz von *DRMS* die im Urheberrecht verankerten Schrankenregelungen ausgehebelt werden.<sup>521</sup>
- 217 Diese Befürchtungen sind insoweit zu relativieren, als dass *DRM*-Systeme lediglich die Herstellung einer digitalen Kopie ohne Qualitätseinbußen verhindern bzw. erschweren können.<sup>522</sup> Durch Ausnutzung der sog. analogen Lücke ist die Herstellung von Werkkopien selbst bei *DRM*-geschützten Werken weiterhin möglich.<sup>523</sup> Die analoge Lücke beschreibt das Phänomen, dass jedes digitale Multimediawerk zu irgendeinem Zeitpunkt in einer für die menschlichen Sinne wahrnehmbaren Form, z.B. auf einem Bildschirm, angezeigt oder über Lautsprecher wiedergegeben werden muss (analoge Wie-

---

<sup>519</sup> Vgl. dazu <[https://de.wikipedia.org/wiki/Digitale\\_Rechteverwaltung#Technische\\_Umsetzung](https://de.wikipedia.org/wiki/Digitale_Rechteverwaltung#Technische_Umsetzung)> (besucht 25. August 2015); FITZNER, 53 ff.

<sup>520</sup> HAUNREITER, 107; SCHULZ, GRUR 2006, 472; HILTY, ZUM 2003, 998.

<sup>521</sup> HAUNREITER, 107; so verunmöglicht ein *DRM*-System auch die Herstellung einer nach Art. 19 Abs. 1 lit. a URG zulässigen Werkkopie zum Eigengebrauch (z.B. als Sicherungszweck); HILTY, Urheberrecht, Rz. 431; PEUKERT, sic! 2004, verweist zudem auf die Problematik der Doppelvergütungen „bei unverändertem Nebeneinander von Pauschalvergütung und zulässigem Einsatz von *DRM*“.

<sup>522</sup> Kritisch BECHTOLD, Informationsrecht, 381 f., ist der Ansicht, dass es problematisch erscheint, „einen Nutzer, der von urheberrechtlichen Schrankenbestimmungen Gebrauch machen will, auf technisch inferiore Versionen des Inhalts zu verweisen“.

<sup>523</sup> FITZNER, 85; JANISCH/LACHENMANN, MMR 2013, 215.

dergabe).<sup>524</sup> Dabei können *DRM*-Systeme nicht verhindern, dass diese analogen Signale durch externe Geräte (Mikrofone, Filmkameras etc.) aufgenommen und zu einem späteren Zeitpunkt durch Verwendung bestimmter Programme (re-)digitalisiert und gegebenenfalls weiterverbreitet werden.<sup>525</sup> Durch Verwendung gewisser Computerprogramme ist es zudem möglich, dass die geschützten Daten während der Werkwiedergabe direkt am analogen Ausgang der Soundkarte aufgezeichnet werden bzw. dass die Film- und Tonspur während des Abspielvorgangs aufgenommen wird.<sup>526</sup>

#### **4. Rechtlicher Schutz technischer Massnahmen (Art. 39a URG)**

##### **A. Allgemeines**

Art. 39a URG statuiert, in Umsetzung von Art. 11 WCT und Art. 18 WPPT, ein Verbot der Umgehung technischer Massnahmen zum Schutz von Werken und anderen Schutzobjekten (Abs. 1).<sup>527</sup> Geschützt werden Werke und geschützte Leistungen i.S.d. URG.<sup>528</sup> Unter den Begriff der technischen Massnahmen fällt jedes technische Mittel, das bestimmt und geeignet ist, um unerlaubte Verwendungen von Werken und anderen Schutzobjekten zu verhindern oder einzuschränken (Abs. 2). Die Bestimmung pönalisiert zudem auch Vorbereitungshandlungen zur Umgehung technischer Massnahmen (Abs. 3). Um eine überschüssende Wirkung der Bestimmung zu verhindern, wurde ein Vorbehalt zugunsten erlaubter Verwendungen in das Gesetz aufgenommen (Abs. 4). Dadurch soll der im digitalen Umfeld besonders schwierig und anspruchsvoll zu handhabende Interessenausgleich zwischen den Urhebern, Verwertern und Nutzern sichergestellt werden.<sup>529</sup>

---

<sup>524</sup> FITZNER, 85; BAUMGARTNER, 164 ff.

<sup>525</sup> JANISCH/LACHENMANN, MMR 2013, 215; BECHTOLD, Informationsrecht, 381.

<sup>526</sup> JANISCH/LACHENMANN, MMR 2013, 215, da die technischen Schutzmassnahmen nicht mitkopiert werden, liegt am Ende eine *DRM*-freie Werkkopie vor.

<sup>527</sup> THOUVENIN, ACTA, 119; AUF DER MAUR, SHK URG, Art. 39a N 2; HAUNREITER, 115; BARRELET/EGLOFF, Art. 39a N 3.

<sup>528</sup> AUF DER MAUR, SHK URG, Art. 39a N 3; HILTY, Urheberrecht, Rz. 431 f.; HAUNREITER, 115 f.; BARRELET/EGLOFF, Art. 39a N 3; Botschaft URG 2006, 3424.

<sup>529</sup> MEYER/GOVONI, SIWR II/1, 415, lehnen es ab, bei einer die Privatkopie verunmöglichenden Kopiersperre von einer überschüssenden Wirkung i.S.d. Gesetzes zu sprechen, weil die Schrankenregelung zum Eigengebrauch dem Schutz der Privatsphäre

- 219 Die Umgehung einer technischen Massnahme ist nur dann strafbar, wenn diese vorsätzlich und unrechtmässig erfolgt ist.<sup>530</sup> PLATZ weist deshalb zu Recht darauf hin, dass der betreffende Nutzer zunächst überhaupt Notiz von der technischen Schutzvorrichtung nehmen muss, damit das subjektive Tatbestandsmerkmal des Vorsatzes gegeben ist.<sup>531</sup>

## **B. Umgehungsverbot (Abs. 1)**

- 220 Die Umgehungshandlung ist dadurch charakterisiert, dass der Täter eine geeignete Sicherheitsvorkehrung umgeht.<sup>532</sup> Die Art und Weise, wie der Täter die Vorkehrung umgeht bzw. unbrauchbar macht (bspw. durch Hacking, Ausspähen des Passworts etc.) ist nicht entscheidend, sondern einzig der Umstand, dass er eine Schranke überwindet, die dazu bestimmt und geeignet ist, eine unrechtmässige Verwendung des Werks zu verhindern.<sup>533</sup>

## **C. Wirksame technische Massnahme (Abs. 2)**

- 221 Als wirksame technische Massnahmen i.S.v. Art. 39a Abs. 2 URG gelten sämtliche „Technologien und Vorrichtungen wie Zugangs- und Kopierkontrollen, Verschlüsselungs-, Verzerrungs- und andere Umwandlungsmechanismen, welche bestimmt und geeignet sind, unerlaubte Verwendungen von Werken und anderen Schutzobjekten zu verhindern oder einzuschränken“. Es handelt sich dabei um eine beispielhafte, nicht abschliessende Aufzählung von Umgehungsmitteln und -verfahren.<sup>534</sup> Nach dem Wortlaut der Bestimmung wird unzweideutig gefordert, dass die technische Massnahme zur Verhinderung von unerlaubten Verwendungen von Werken und anderen Schutzobjekten bestimmt und geeignet sein muss, weshalb es nicht ausreicht, wenn diese bloss den urheberrechtlich nicht geschützten Werkgenuss verhindern.<sup>535</sup> Es muss jeweils im Einzelfall geprüft werden, ob durch die technische Massnahme tatsächlich eine unerlaubte Werkverwendung verhindert wird.

---

dient und „nicht dem Ziel, Privatkopien zu ermöglichen“; AUF DER MAUR, SHK URG, Art. 39a N 14; HILTY, Urheberrecht, Rz. 433 f.; Botschaft URG 2006, 3426.

<sup>530</sup> AUF DER MAUR, SHK URG, Art. 39a N 4; REHBINDER/VIGANÒ, Art. 39a N 12; PLATZ, Jusletter vom 16. Juni 2008, Rz. 3.

<sup>531</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 4.

<sup>532</sup> AUF DER MAUR, SHK URG, Art. 39a N 1.

<sup>533</sup> AUF DER MAUR, SHK URG, Art. 39a N 1; BARRELET/EGLOFF, Art. 39a N 6.

<sup>534</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 3.

<sup>535</sup> MEYER/GOVONI, SIWR II/1, 416; BARRELET/EGLOFF, Art. 39a N 8.

Die Anforderungen an die Wirksamkeit der technischen Massnahmen sollten 222 nach Ansicht von REHBINDER/VIGANÒ nicht zu hoch angesetzt werden, da eine vollumfängliche Sicherheit gegen jegliche Angriffsmöglichkeiten nie realisiert werden könne.<sup>536</sup> Deshalb schlagen diese Autoren vor, dass ein ausreichender Schutz bereits dann als gegeben angenommen werden sollte, wenn die Massnahmen geeignet sind, den Durchschnittskonsumenten davon abzuhalten, eine Handlung vorzunehmen, die bestimmungsgemäss verhindert werden soll.<sup>537</sup> Gemäss der Botschaft des Bundesrates werden nur diejenigen technischen Massnahmen rechtlich geschützt, die einen Mindestschutz bieten.<sup>538</sup> AUF DER MAUR will den rechtlichen Schutz selbst dann nicht beseitigt sehen, wenn eine Umgehungsmöglichkeit für eine Schutzmassnahme bekannt ist.<sup>539</sup> PLATZ spricht sich dafür aus, jene Schutzmassnahmen für wirksam und geeignet zu erklären, die von einem Durchschnittskonsumenten nicht ohne den Einsatz von Vorrichtungen nach Art. 39a Abs. 3 URG umgangen werden können.<sup>540</sup>

Letztlich muss einzelfallabhängig entschieden werden, ob eine technische 223 Massnahme die vom Gesetz geforderte Wirksamkeit erreicht oder nicht. Wenn ein Durchschnittskonsument eine technische Massnahme mit wenigen Mausklicks umgehen kann oder falls entsprechende Umgehungswerkzeuge im Internet weit verbreitet sind, sollte nach hier vertretener Ansicht das Vorliegen einer wirksamen technischen Massnahme eher zurückhaltend bejaht werden.

#### D. Verbot von Vorbereitungshandlungen (Abs. 3)

Nebst der Umgehung einer wirksamen technischen Schutzmassnahme wer- 224 den in Art. 39a Abs. 3 URG zahlreiche Vorbereitungshandlungen unter Strafe gestellt.<sup>541</sup> Vom Verbot werden sämtliche (mechanischen sowie elektroni-

<sup>536</sup> REHBINDER/VIGANÒ, Art. 39a N 13.

<sup>537</sup> AUF DER MAUR, SHK URG, Art. 39a N 2; REHBINDER/VIGANÒ, Art. 39a N 13; BARRELET/EGLOFF, Art. 39a N 8.

<sup>538</sup> Botschaft URG 2006, 3414, 3424 f.

<sup>539</sup> AUF DER MAUR, SHK URG, Art. 39a N 2.

<sup>540</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 9.

<sup>541</sup> AUF DER MAUR, SHK URG, Art. 39a N 6; HAUNREITER, 117, weist darauf hin, dass die Regelung von Art. 39a Abs. 3 URG – durch die Pönalisierung blosser Vorbereitungshandlungen zur Umgehung technischer Massnahmen – über die Vorgaben von Art. 11 WCT und Art. 18 WPPT hinausgeht; HILTY, Urheberrecht, Rz. 432, wendet ein, dass das Programm oder das Erbringen einer entsprechenden Dienstleistung nur dann dem Ver-

schen) Vorrichtungen, Erzeugnisse oder Bestandteile erfasst, die geeignet sind, die Wirksamkeit technischer Schutzmassnahmen teilweise oder ganz zu beseitigen.<sup>542</sup> Nach dem Wortlaut des Gesetzes wird für das Verbot zudem vorausgesetzt, dass die Umgehungswerkzeuge – abgesehen von der Umgehung technischer Schutzmassnahmen – nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben.<sup>543</sup> Durch die Pönalisierung von Vorbereitungshandlungen zur Umgehung technischer Massnahmen nach Art. 39a Abs. 3 und Art. 69a Abs. 1 lit. b URG sollen die Verbreitung von Umgehungswerkzeugen sowie das Erbringen von Dienstleistungen, die im Zusammenhang mit der Umgehung technischer Massnahmen stehen, unterbunden werden.<sup>544</sup> Die Schaffung selbständiger Vorbereitungsdelikte ermöglicht eine strafrechtliche Bekämpfung von Teilnahmehandlungen, welche bereits vor dem Versuchsstadium der Haupttat stattfinden.<sup>545</sup> Dadurch soll den Rechteinhabern ein wirksames Instrument zur Kontrolle von Vorrichtungen und Dienstleistungen gegeben werden, welche eine Umgehung der technischen Schutzmassnahmen überhaupt erst ermöglichen.<sup>546</sup>

#### **E. Vorbehalt erlaubter Verwendungen (Abs. 4)**

- 225 Art. 39a Abs. 4 URG statuiert, dass das Umgehungsverbot nicht geltend gemacht werden kann, wenn die Umgehung ausschliesslich zum Zwecke einer erlaubten Verwendung erfolgt (insbesondere für Privat- und Sicherungskopien nach Art. 19 Abs. 1 lit. a bzw. Art. 24 Abs. 1 URG).<sup>547</sup> Folglich greift das Umgehungsverbot von Art. 39a Abs. 1 URG nur dann, wenn durch die Umgehung einer technischen Massnahme tatsächlich eine Urheber-

---

bot unterliegt, wenn die Zweckbestimmung überwiegend in der Umgehung von technischen Schutzmassnahmen liegt; BARRELET/EGLOFF, Art. 39a N 9; REHBINDER/VIGANÒ, Art. 39a N 15 ff.

<sup>542</sup> BARRELET/EGLOFF, Art. 39a N 10; REHBINDER/VIGANÒ, Art. 39a N 18.

<sup>543</sup> MEYER/GOVONI, SIWR II/1, 418; BARRELET/EGLOFF, Art. 39a N 11; REHBINDER/VIGANÒ, Art. 39a N 20 f.

<sup>544</sup> RUBLI, Rz. 335; HAUNREITER, 117; Botschaft URG 2006, 3425.

<sup>545</sup> RUBLI, Rz. 336.

<sup>546</sup> AUF DER MAUR, SHK URG, Art. 39a N 6; RUBLI, Rz. 336; BARRELET/EGLOFF, Art. 39a N 9 ff.

<sup>547</sup> AUF DER MAUR, SHK URG, Art. 39a N 14; BARRELET/EGLOFF, Art. 39a N 12; REHBINDER/VIGANÒ, Art. 39a N 26; PLATZ, Jusletter vom 16. Juni 2008, Rz. 6.

rechtsverletzung begangen wird.<sup>548</sup> Diese Regelung soll verhindern, dass der Umgehungsschutz eine überschüssende Wirkung gegenüber den Schrankenregelungen des Urheberrechts erhält.<sup>549</sup>

Gemäss Botschaft ist ein Eingriff in technische Massnahmen zwar grundsätzlich verboten, aber seine Verletzung hat weder zivil- noch strafrechtliche Konsequenzen, wenn der Eingriff ausschliesslich dem Zweck gedient hat, eine gesetzlich erlaubte Verwendung des Schutzobjekts vorzunehmen.<sup>550</sup> Gesetzlich erlaubt ist eine Verwendung, die unter eine Schutzschranke (Art. 19 ff. URG) fällt, Werke betrifft, die gemäss Art. 5 URG vom Urheberrechtsschutz ausgenommen sind oder sich auf Werke und Leistungen bezieht, deren Schutzfrist bereits abgelaufen ist.<sup>551</sup>

Nach REHBINDER/VIGANÒ verhindert Art. 39a Abs. 4 URG einzig, dass die Verbotsfolgen durchgesetzt werden können (Prozessvoraussetzung). Eine gesetzliche Erlaubnis zur Umgehung technischer Massnahmen sei hingegen in dieser Bestimmung nicht enthalten.<sup>552</sup> Dies hat nach Ansicht dieser Autoren zur Folge, dass die nicht sanktionierbare Umgehung unrechtmässig bleibt und Art. 39a Abs. 4 URG nicht als Rechtfertigungsgrund herangezogen werden kann, wenn mit der Umgehung zugleich ein anderer Verbotstatbestand, bspw. Art. 39a Abs. 3 URG, Art. 39c URG oder ein Straftatbestand nach StGB erfüllt ist.<sup>553</sup> AUF DER MAUR ist der Meinung, dass der Vorbehalt von Art. 39a Abs. 4 URG lediglich die Durchsetzbarkeit ausschliesst und die Umgehung technischer Massnahmen grundsätzlich unrechtmässig bleiben, weshalb diese Bestimmung nicht als Rechtfertigungsgrund nach Art. 14 StGB herangezogen werden könne.<sup>554</sup>

Aus der missverständlichen Formulierung in der Botschaft, dass Eingriffe in technische Massnahmen zwar „grundsätzlich verboten“ seien, kann m.E. nicht gefolgert werden, dass die nicht sanktionierbare Umgehung unrecht-

---

<sup>548</sup> MEYER/GOVONI, SIWR II/1, 416; HAUNREITER, 119; BARRELET/EGLOFF, Art. 39a N 12; REHBINDER/VIGANÒ, Art. 39a N 26.

<sup>549</sup> AUF DER MAUR, SHK URG, Art. 39a N 14; Botschaft URG 2006, 3424.

<sup>550</sup> Botschaft URG 2006, 3425.

<sup>551</sup> AUF DER MAUR, SHK URG, Art. 39a N 15; HAUNREITER, 119; BARRELET/EGLOFF, Art. 39a N 12; Botschaft URG 2006, 3425.

<sup>552</sup> REHBINDER/VIGANÒ, Art. 39a N 26.

<sup>553</sup> REHBINDER/VIGANÒ, Art. 39a N 26.

<sup>554</sup> AUF DER MAUR, SHK URG, Art. 39a N 19; ebenso BARRELET/EGLOFF, Art. 39a N 12, die davon sprechen, dass die Umgehung aufgrund von Art. 39a Abs. 1-3 URG eine unerlaubte Handlung bleibt.

mässig bleiben würde. Ansonsten würde ein paradoxer Zustand geschaffen, indem einerseits ein Verhalten für unrechtmässig erklärt wird, dessen Sanktionierung andererseits ausgeschlossen wird. Indem Art. 39a Abs. 4 URG statuiert, dass die „Umgehung ausschliesslich zum Zwecke einer gesetzlich erlaubten Verwendung“ weder zivil- noch strafrechtlich geahndet wird, ist nach hier vertretener Ansicht ein Rechtfertigungsgrund zugunsten genau dieser „gesetzlich erlaubten Verwendungen“ zu sehen.<sup>555</sup> Eine gerechtfertigte Handlung kann definitionsgemäss nicht unrechtmässig sein, da die Widerrechtlichkeit durch das Vorliegen des Rechtfertigungsgrundes aufgehoben wird. Die Tragweite des Art. 39a Abs. 4 URG ist insoweit einzuschränken, als nur Fälle der Umgehung von Nutzungsschranken nach Art. 39a Abs. 1 URG von diesem Vorbehalt umfasst werden.<sup>556</sup> Eine etwaige Bestrafung wegen Vorbereitungshandlungen nach Art. 39a Abs. 3 i.V.m. Art. 69a Abs. 1 lit. b URG sowie wegen einschlägiger Computerstraftatbestände nach StGB bei der Umgehung wirksamer Zugangsschranken, wird dadurch nicht ausgeschlossen.<sup>557</sup> Der Vorbehalt von Art. 39a Abs. 4 URG gilt sodann nur für den Berechtigten selbst und nicht auch für Mittäter, Anstifter oder Gehilfen.<sup>558</sup>

---

<sup>555</sup> Ebenso SCHWARZENEGGER, ZSR 2008 II, 498, m.w.H.; unklar GLARNER, sic! 2006, 649 f.; widersprüchlich BARRELET/EGLOFF, Art. 39a N 12, welche die Umgehung zwar einerseits als eine „unerlaubte Handlung“ qualifizieren, sodann aber präzisieren, dass die Umgehung nicht widerrechtlich sei, wenn sie „ausschliesslich einer unter eine Schutz Ausnahme fallenden Nutzung dient“.

<sup>556</sup> Bei der Umgehung einer wirksamen Zugangsschranke kann sich ein Nutzer m.E. nicht auf die in Art. 19 Abs. 1 lit. a URG statuierte Schrankenregelung zum Eigengebrauch berufen. Letztgenannte Bestimmung bezieht sich ausschliesslich auf Werkverwendungen. Die Umgehung einer Zugangsschranke zu geschützten Werken stellt indessen keine Werkverwendung dar, sondern eine Beschaffungshandlung. Von einer Werkverwendung kann erst dann gesprochen werden, wenn ein Nutzer faktisch bereits den Zugriff auf das Werk innehat. Dies ist bei der Umgehung von Zugangsschranken gerade nicht der Fall. Ein Recht zur Umgehung von Zugangsschranken kann aus Art. 39a Abs. 4 i.V.m. Art. 19 Abs. 1 lit. a URG nicht abgeleitet werden.

<sup>557</sup> Vgl. AUF DER MAUR, SHK URG, Art. 39a N 18 ff.; RUBLI, Rz. 454; REHBINDER/VIGANÒ, Art. 39a N 26; a.A. SCHWARZENEGGER, ZSR 2008 II, 498 f., wonach sich die Rechtmässigkeit der Umgehung (einer Zugangssicherung) zum Zwecke einer gesetzlich erlaubten Verwendung nach Art. 14 StGB auch auf die unbefugte Datenbeschaffung nach Art. 143 StGB überträgt.

<sup>558</sup> AUF DER MAUR, SHK URG, Art. 39a N 16; REHBINDER/VIGANÒ, Art. 39a N 27.



## **5. Verletzung des Schutzes von technischen Massnahmen und von Informationen für die Wahrnehmung von Rechten (Art. 69a URG)**

### **A. Allgemeines**

Der Tatbestand von Art. 69a URG wurde im Jahr 2008 neu eingeführt für<sup>229</sup> den Fall der Verletzung technischer Schutzmassnahmen (Art. 39a URG) bzw. im Zusammenhang mit der Entfernung oder Änderung elektronischer Informationen zur Wahrnehmung der Schutzrechte (Art. 39c URG).<sup>559</sup> Massgebend für die Anwendung dieser Strafbestimmung sind die allgemeinen Vorschriften des Strafgesetzbuches (Art. 333 StGB).<sup>560</sup> Geschützte Rechtsgüter sind die Urheberrechte und die verwandten Schutzrechte. Die technischen Massnahmen werden nur soweit geschützt, als sie dem Schutz der Urheberrechte und verwandten Schutzrechte dienen.<sup>561</sup> Der Rechtsschutz ist dabei auf Gefährdungshandlungen im Vorfeld der eigentlichen Verletzung der geschützten Rechtsgüter gerichtet.<sup>562</sup>

### **B. Umgehung technischer Massnahmen**

Die Strafbestimmung von Art. 69a Abs. 1 lit. a URG versieht das Umge-<sup>230</sup> hungsverbot von Art. 39a Abs. 1 URG mit einer Strafandrohung.<sup>563</sup> Falls die Umgehung einer wirksamen technischen Massnahme mit der Absicht vorgenommen wird, eine gesetzlich unerlaubte Verwendung von Werken oder anderen Schutzobjekten vorzunehmen, wird der Täter mit Busse bestraft. Aufgrund der individualrechtlichen Ausgestaltung des Rechtsschutzes im URG ist die Strafbarkeit gemäss Art. 69a Abs. 1 URG an einen Strafantrag gebunden, wobei die Antragsbefugnis – nach dem Grundsatz von Art. 30 Abs. 1 StGB – jedem materiell-rechtlichen Träger des verletzten Rechtsgutes

---

<sup>559</sup> BÖTTCHER, 240 f.; DAVID, SHK URG, Art. 69a N 2; HILTY, Urheberrecht, Rz. 425; BARRELET/EGLOFF, Art. 69a N 1; REHBINDER/VIGANÒ, Art. 69a N 1; GLARNER, sic! 2006, 647 f.; ders., Musikpiraterie im Internet, 42.

<sup>560</sup> BARRELET/EGLOFF, Art. 69a N 2; SCHWARZENEGGER, ZSR 2008 II, 462.

<sup>561</sup> BARRELET/EGLOFF, Art. 69a N 3; REHBINDER/VIGANÒ, Art. 69a N 1; GLARNER, sic! 2006, 650.

<sup>562</sup> REHBINDER/VIGANÒ, Art. 69a N 1, die ebenfalls von einem konkreten Gefährungsdelikt ausgehen; ebenso SCHWARZENEGGER, ZSR 2008 II, 464; a.A. GLARNER, sic! 2006, 648, der von einem abstrakten Gefährungsdelikt ausgeht.

<sup>563</sup> REHBINDER/VIGANÒ, Art. 69a N 6.

zukommt.<sup>564</sup> Hierzu zählen sämtliche Personen, welche „*die betroffenen Urheber- und verwandten Schutzrechte in eigenem Namen geltend machen können*“<sup>565</sup>.<sup>566</sup> Weiter muss die Tat unrechtmässig, d.h. gegen den Willen des Trägers des geschützten Rechtsgutes bzw. ohne Einwilligung der Rechteinhaber oder Exklusivlizenznehmer erfolgt sein.<sup>567</sup>

- 231 In subjektiver Hinsicht setzt der Straftatbestand eine vorsätzliche Tatbegehung voraus, wobei Eventualvorsatz genügt.<sup>568</sup> Der Täter muss zudem mit der Absicht handeln, eine gesetzlich unerlaubte Verwendung von Werken oder anderen Schutzobjekten vorzunehmen.<sup>569</sup> Die Umgehung wirksamer technischer Massnahmen im Hinblick auf erlaubte Werkverwendungen, insbesondere zum Eigengebrauch, ist nicht strafbar.<sup>570</sup> REHBINDER/VIGANÒ sprechen diesbezüglich von einer „überschiessenden Innentendenz“<sup>571</sup>.

### **C. Beschaffung, Herstellung und Vertrieb von Vorrichtungen zur Umgehung technischer Massnahmen**

- 232 In Übereinstimmung mit Art. 39a Abs. 3 URG stellt Art. 69a Abs. 1 lit. b URG bestimmte Vorbereitungshandlungen unter Strafe, die den Zugang zu Vorrichtungen, Erzeugnissen oder Bestandteilen erleichtern, welche der Umgehung wirksamer technischer Massnahmen dienen.<sup>572</sup> Die Vorbereitungshandlungen nach lit. b sind – im Unterschied zur Umgehungshandlung nach

---

<sup>564</sup> DAVID, SHK URG, Art. 69a N 5; BARRELET/EGLOFF, Art. 69a N 1; REHBINDER/VIGANÒ, Art. 69a N 2; SCHWARZENEGGER, ZSR 2008 II, 490 f., m.w.H.

<sup>565</sup> REHBINDER/VIGANÒ, Art. 69a N 6.

<sup>566</sup> DAVID, SHK URG, Art. 69a N 5, weist darauf hin, dass primär sowohl die Rechteinhaber als auch die ausschliesslichen Lizenznehmer antragsberechtigt sind; BARRELET/EGLOFF, Art. 69a N 3; GLARNER, sic! 2006, 650.

<sup>567</sup> GLARNER, Musikpiraterie im Internet, 76f.; SCHWARZENEGGER, ZSR 2008 II, 463; ders., Urheberstrafrecht, 205 ff., 218.

<sup>568</sup> BARRELET/EGLOFF, Art. 69a N 5; REHBINDER/VIGANÒ, Art. 69a N 4.

<sup>569</sup> DAVID, SHK URG, Art. 69a N 7b; BARRELET/EGLOFF, Art. 69a N 6; REHBINDER/VIGANÒ, Art. 69a N 7.

<sup>570</sup> DAVID, SHK URG, Art. 69a N 7b; BARRELET/EGLOFF, Art. 69a N 6; REHBINDER/VIGANÒ, Art. 69a N 7.

<sup>571</sup> REHBINDER/VIGANÒ, Art. 69a N 7.

<sup>572</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 22; BARRELET/EGLOFF, Art. 69a N 7; REHBINDER/VIGANÒ, Art. 69a N 8; SCHWARZENEGGER, ZSR 2008 II, 464.

lit. a – auch dann strafbar, wenn sie im Hinblick auf eine gesetzlich erlaubte Verwendung erfolgen.<sup>573</sup>

Obschon Art. 69a Abs. 1 lit. b URG als abstraktes Gefährdungsdelikt ausgestaltet wurde, ist auch diese Tatbestandsvariante als Antragsdelikt konzipiert.<sup>574</sup> Die Verknüpfung eines Antragsdelikts mit einem abstrakten Gefährdungsdelikt ist problematisch, da zu diesem Zeitpunkt noch gar nicht feststeht, welcher Rechteinhaber von der Vorbereitungshandlung betroffen ist.<sup>575</sup> Die Tatbestandsvarianten von Art. 69a Abs. 1 lit. b URG hätten richtigerweise „als Offizialdelikte definiert werden müssen“<sup>576</sup>. Damit diese Bestimmung nicht toter Buchstabe bleibt, wird vorgeschlagen, jeden potentiell betroffenen Urheber oder sonstigen Leistungsschutzberechtigten als antragsberechtigt anzusehen.<sup>577</sup>

## D. Gewerbsmässige Verletzung

Die gewerbsmässige Verletzung von technischen Massnahmen und von Informationen zur Rechtswahrnehmung ist als Offizialdelikt ausgestaltet und wird von Amtes wegen verfolgt (Art. 69a Abs. 2 URG).<sup>578</sup> Der Strafraum beträgt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.

## 6. Umgehung von Zugangsschranken bei kostenpflichtigen Streaming-Angeboten

### A. Fallbeispiel

Das populäre Videostreaming-Portal *Netflix*<sup>579</sup> bietet seinen Kunden gegen Bezahlung einer monatlichen Gebühr den uneingeschränkten Zugriff auf

---

<sup>573</sup> DAVID, SHK URG, Art. 69a N 11; REHBINDER/VIGANÒ, Art. 69a N 8.

<sup>574</sup> DAVID, SHK URG, Art. 69a N 9, plädiert *de lege ferenda* für eine Ausgestaltung als Offizialdelikt aus, damit der Staat „von sich aus eingreifen [kann], wenn solche Geräte angetroffen werden“; vgl. dazu auch REHBINDER/VIGANÒ, Art. 69a N 8; SCHWARZENEGGER, ZSR 2008 II, 464; GLARNER, sic! 2006, 648.

<sup>575</sup> REHBINDER/VIGANÒ, Art. 69a N 2; SCHWARZENEGGER, ZSR 2008 II, 464 f.

<sup>576</sup> SCHWARZENEGGER, ZSR 2008 II, 491.

<sup>577</sup> Ebenso MEYER/GOVONI, SIWR II/1, 419; REHBINDER/VIGANÒ, Art. 69a N 2; SCHWARZENEGGER, ZSR 2008 II, 491.

<sup>578</sup> DAVID, SHK URG, Art. 69a N 19; BARRELET/EGLOFF, Art. 69a N 12; REHBINDER/VIGANÒ, Art. 69a N 11; PLATZ, Jusletter vom 16. Juni 2008, Rz. 5.

<sup>579</sup> <<https://www.netflix.com/ch>> (besucht 25. August 2015).

eine grosse Zahl von Serien und Filmen. Damit ein Kunde auf die kostenpflichtigen Angebote zugreifen kann, muss er zuvor eine passwortgesicherte Zugangskontrolle passieren. Ein Nutzer überwindet diese Zugangsschranke auf eine nicht näher zu spezifizierende Weise und verschafft sich – ohne Bezahlung des geforderten Entgelts – den Zugang zu einem kostenpflichtigen Streaming-Angebot, welches sodann abgerufen und konsumiert wird.

## **B. Umgehungshandlung**

- <sup>236</sup> Die Umgehungshandlung ist dadurch charakterisiert, dass der Täter eine geeignete Sicherheitsvorkehrung umgeht. Die Art und Weise, wie der Täter die technische Massnahme umgeht bzw. unbrauchbar macht, ist nicht entscheidend, sondern einzig der Umstand, dass er eine Schranke überwindet, die geeignet und dazu bestimmt ist, eine unrechtmässige Verwendung zu verhindern.<sup>580</sup> Sobald sich ein Nutzer ohne Einwilligung der Rechteinhaber und unter Umgehung einer wirksamen technischen Massnahme Zugang zu einem urheberrechtlich geschützten Werk verschafft, ist eine Umgehungshandlung i.S.v. Art. 69a Abs. 1 lit. a URG zu bejahen.

## **C. Rechtliche Bewertung der Umgehung von Zugangsschranken zur Entgeltsicherung nach URG**

- <sup>237</sup> Der Einsatz von Zugangsschranken ermöglicht es den Anbietern festzulegen, unter welchen Voraussetzungen einem Nutzer der Zugriff auf die geschützten Inhalte eingeräumt werden soll.<sup>581</sup> Der Hauptzweck der Zugangskontrollsysteme besteht darin zu verhindern, dass ein Nutzer ohne die Einwilligung des Anbieters – die zumeist von der Entrichtung eines Entgelts abhängig gemacht wird – Zugriff auf die geschützten Daten erhält. Die Zugangsschranken schützen regelmässig nicht primär vor einer unrechtmässigen Datenverwendung, welche Art. 69a URG zu verhindern anstrebt, sondern das Vermögen des Anbieters.<sup>582</sup> Die Verhinderung der unrechtmässigen Datenverwendung stellt eine bloss mittelbare Begleiterscheinung dar.

---

<sup>580</sup> DAVID, SHK URG, Art. 69a N 8b; RUBLI, Rz. 26 ff.

<sup>581</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 26 f.; GLARNER, sic! 2006, 643.

<sup>582</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 4, wonach es sich beim geschützten Rechtsgut von Art. 39a URG indirekt um das Vermögen handelt; GLARNER, sic! 2006, 649 f., vertritt die Ansicht, dass die Aufnahme der Zugangsschranken in den Katalog von Art. 39a

Bei der urheberstrafrechtlichen Bewertung einer Umgehung wirksamer technischer Massnahmen nach Art. 39a Abs. 2 URG muss sodann geprüft werden, ob sich der Nutzer bei der Umgehung auf die Schranke zugunsten des Privatgebrauchs nach Art. 19 Abs. 1 lit. a i.V.m. Art. 39a Abs. 4 URG stützen kann.<sup>583</sup>

Ein Teil der Schweizer Lehre vertritt die Ansicht, dass sich ein Nutzer nicht auf die Schrankenregelung zugunsten des Eigengebrauchs nach Art. 19 Abs. 1 lit. a URG berufen können soll, wenn der Zugang zum urheberrechtlich geschützten Werk mit einer wirksamen technischen Zugangsschranke versehen war, welche der Nutzer vorab umgehen oder ausschalten musste.<sup>584</sup> Durch Art. 19 Abs. 1 lit. a URG werde den Nutzern kein Zugriffs-, sondern lediglich ein Nutzungsrecht verliehen. Folglich könne sich ein Nutzer erst dann auf die Schrankenregelung zum Privatgebrauch berufen, wenn sich das urheberrechtlich geschützte Werk bereits im Verfügungsbereich des Nutzers befindet.<sup>585</sup>

Teilweise wird auch die Meinung vertreten, dass durch die Aufnahme von Zugangskontrollsystemen als taugliche Tatobjekte von Art. 69a URG die Ausgestaltung der gesetzlichen Lizenzen neu definiert würde. Ein Nutzer würde demnach nicht tatbestandsmässig i.S.v. Art. 69a Abs. 1 lit. a URG handeln, wenn er sich bei der Umgehung einer Zugangsschranke auf eine Schutzschranke berufen könne. Somit würde Art. 19 URG von einem ausschliesslichen Verwendungsrecht zu einem eigentlichen Zugriffsrecht mutieren.<sup>586</sup>

Letzterer Ansicht kann m.E. nicht gefolgt werden. Die Schrankenregelung von Art. 19 URG trägt den Titel „Verwendung zum Eigengebrauch“ und bestimmt, welche Verwendungen im Rahmen des Eigengebrauchs an veröffentlichten Werken vorgenommen werden dürfen. Bei der Umgehung einer Zugangsschranke handelt es sich nicht um eine Werkverwendung zum Eigengebrauch, sondern um die unerlaubte Verschaffung des Zugriffs auf ge-

---

Abs. 2 URG ungerechtfertigt sei und deren Umgehung richtigerweise nur den Strafnormen des StGB unterstellt werden sollten.

<sup>583</sup> HAUNREITER, 116; SCHWARZENEGGER, ZSR 2008 II, 494.

<sup>584</sup> GASSER, SHK URG, Art. 19 N 10b; BARRELET/EGLOFF, Art. 19 N 7b; GLARNER, sic! 2006 643, m.w.H.; GASSER, 61 f.; a.A. SCHWARZENEGGER, ZSR 2008 II, 494, der die Ansicht vertritt, dass die Schrankenregelung zum Eigengebrauch auch bei der Umgehung von Zugangsschranken tatbestandsausschliessende Wirkung habe.

<sup>585</sup> Zum Ganzen GLARNER, sic! 2006, 643.

<sup>586</sup> Zum Ganzen GLARNER, sic! 2006, 649.

geschützte Werke. Eine „Werkverwendung zum Eigengebrauch“ liegt nur dann vor, wenn sich die Daten bereits in der Verfügungsgewalt des Nutzers selbst oder einer mit dem Nutzer eng verbundenen Person befinden. Die Beschaffung unter Umgehung einer Zugangsschranke stellt eine der Verwendungshandlung (zeitlich) vorgelagerte Beschaffungshandlung dar, die es klar von dieser zu unterscheiden gilt und die folglich nicht unter die Schrankenregelung von Art. 19 URG subsumiert werden kann. Eine Berufung auf die Schrankenregelung für die Verwendung zum Eigengebrauch nach Art. 19 URG ist deshalb ausgeschlossen, wenn der Zugriff zu den geschützten Inhalten unter Umgehung einer wirksamen Zugangsschranke beschafft worden ist. Eine Ausdehnung des in Art. 19 Abs. 1 lit. a URG verankerten Verwendungsrechts zugunsten des Privatgebrauchs hin zu einem Zugriffsrecht ist abzulehnen.<sup>587</sup>

- 242 Aufgrund der missglückten Formulierung wird eine Strafbarkeit nach Art. 69a Abs. 1 lit. a URG aber gleichwohl regelmässig zu verneinen sein, weil letztgenannter Artikel ausdrücklich festhält, dass nur derjenige bestraft wird, der „*vorsätzlich und unrechtmässig wirksame technische Massnahmen nach Art. 39a Abs. 2 [URG] mit der Absicht umgeht, eine gesetzlich unerlaubte Verwendung von Werken und anderen Schutzobjekten vorzunehmen*“. Sofern ein Nutzer, der sich den Zugang zum Werk unter Umgehung einer Zugangsschranke beschafft hat, nicht mit der Absicht handelt, (anschliessend) eine gesetzlich unerlaubte Verwendung an den rechtswidrig beschafften Daten vorzunehmen, lässt sich dessen Verhalten nicht unter den Tatbestand von Art. 69a Abs. 1 lit. a URG subsumieren.<sup>588</sup> Der Umstand, dass Zugangskontrollen zwar einerseits im „Katalog“ der geschützten technischen Massnahmen enthalten sind, eine Bestrafung nach Art. 69a Abs. 1 lit. a URG in vielen Fällen aber nicht möglich sein wird, rührt daher, dass nicht hinreichend zwischen „Beschaffungshandlungen“ und „Verwendungshandlungen“ differenziert wird. Damit die Umgehung einer Zugangskontrolle nach URG wirksam sanktioniert werden kann, wird hier deshalb vorgeschlagen, Art. 69a Abs. 1 lit. a URG dahingehend zu modifizieren, dass auf Antrag jeder mit Strafe bedroht wird, der vorsätzlich und unrechtmässig eine *technisch wirksame Nutzungsschranke mit der Absicht umgeht, eine gesetzlich*

---

<sup>587</sup> AUF DER MAUR, SHK URG, N 10 Vorb. zu Art. 39a-c, m.w.H.; BARRELET/EGLOFF, Art. 19 N 3, mit dem Hinweis, dass die Schranken des Urheberrechts die Verwendungsrechte betreffen; EGLOFF, *medialex* 2006, 37; AUF DER MAUR/KELLER, *sic!* 2004, 79 ff.; a.A. SCHWARZENEGGER, ZSR 2008 II, 498 f.; GLARNER, *sic!* 2006, 649.

<sup>588</sup> Vgl. SCHWARZENEGGER, ZSR 2008 II, 484 f.

*unerlaubte Verwendung von Werken oder anderen Schutzobjekten vorzunehmen.* In einem neu in das Gesetz aufzunehmenden Art. 69a Abs. 1 lit. a<sup>bis</sup> URG sollte sodann auf Antrag mit Strafe bedroht werden, wer vorsätzlich und unrechtmässig eine *technisch wirksame Zugangsschranke umgeht*.<sup>589</sup>

Andernfalls sollte dem Vorschlag von GLARNER gefolgt werden, der den Schutz technischer Massnahmen in Art. 39a bzw. Art. 69a URG auf Nutzungsschranken einschränken will. Dazu müssten die Zugangskontrollen aus dem Katalog der in Art. 39a Abs. 2 URG aufgeführten geschützten Rechtsgüter gestrichen werden. Die Sanktionierung der Umgehung von Zugangsschranken würde dann ausschliesslich durch die Strafnormen des StGB erfolgen (insbesondere durch Art. 143, Art. 143<sup>bis</sup>, Art. 150 und Art. 150<sup>bis</sup> StGB).<sup>590</sup>

## **D. Rechtliche Bewertung der Umgehung von Zugangsschranken nach StGB**

### **a) Unbefugte Datenbeschaffung (Art. 143 StGB)**

Gemäss wohl h.L. schützt der als Begehungsdelikt konstruierte Art. 143 StGB das ungestörte Verfügungsrecht über Computerdaten sowie das Vermögen.<sup>591</sup> Da bereits mit dem Zugriff auf die Daten das Interesse des Berechtigten tangiert wird, ist Art. 143 StGB als Verletzungsdelikt und nicht als Gefährdungsdelikt zu qualifizieren.<sup>592</sup> Der Tatbestand entspricht weitgehend

---

<sup>589</sup> Kritisch HAUNREITER, 104 f. und GIRSBERGER, 98 f., welche die Ansicht vertreten, dass eine Differenzierung zwischen Zugangs- und Nutzungsschranken nicht immer möglich sei, da viele Abhängigkeiten bestehen.

<sup>590</sup> Zum Ganzen GLARNER, sic! 2006, 650.

<sup>591</sup> WEISSENBERGER, BSK StGB II, Art. 143 N 3 f.; DONATSCH, Strafrecht III, 195, ist der Meinung, dass durch Art. 143 StGB „neben den Vermögensrechten das Verfügungsrecht über die betreffenden Daten geschützt werden“; ähnlich TRECHSEL/CRAMERI, PK StGB, Art. 143 N 2, sehen einen bloss „lockeren Bezug zum Vermögensschutz“; DUPUIS ET AL., Petit Commentaire CP, Art. 143 N 2; einschränkend STRATENWERTH/WOHLERS, Art. 143 N 1, sehen nur das Verfügungsrecht über Computerdaten als geschütztes Rechtsgut; STRATENWERTH/JENNY/BOMMER, § 14 N 23 sehen primär „das Verfügungsrecht an Computerdaten“ als „Immaterialgüterrecht eigener Art“ als geschütztes Rechtsobjekt; GLARNER, Musikpiraterie im Internet, 167, bezeichnet die „formelle Verfügungsmacht über Daten“ als geschütztes Rechtsgut; wiederum anders SCHMID, § 4 N 14 ff., der in der unbefugten Datenbeschaffung vorrangig ein Vermögensdelikt sieht.

<sup>592</sup> WEISSENBERGER, BSK StGB II, Art. 143 N 3 f.; DUPUIS ET AL., Petit Commentaire CP, Art. 143 N 2; SCHWARZENEGGER, FS-Trechsel, 315 f.

demjenigen des Diebstahls nach Art. 139 StGB, mit dem Hauptunterschied, dass als Tatobjekt nicht körperliche Sachen, sondern ausschliesslich unkörperliche Daten in Betracht kommen.<sup>593</sup> Der Datenbegriff umfasst alle Notate, die Gegenstand menschlicher Kommunikation sein können, sofern sie in codierter Form von einer Datenverarbeitungsanlage verarbeitet, gespeichert oder übermittelt werden können.<sup>594</sup> Der objektive Tatbestand setzt voraus, dass der Täter Daten beschafft, die nicht für ihn bestimmt und gegen einen unbefugten Zugriff besonders gesichert sind.<sup>595</sup> Gegen einen unbefugten Zugriff besonders gesichert sind Daten, wenn der Datenberechtigte die zumutbaren und in der konkreten Situation üblichen Massnahmen getroffen hat, um die Daten vor dem unerlaubten Zugriff zu schützen, was i.d.R. bei mechanischen oder elektronischen Zugangssperren anzunehmen ist.<sup>596</sup>

- 245 Nach der wohl h.L. soll Art. 143 StGB nicht auf Schutzvorrichtungen anwendbar sein, die lediglich der Sicherung finanzieller Interessen dienen, sondern nur in jenen Fällen, in denen der Berechtigte grundsätzlich Unbefugten keinen Zugang zu den Daten gewähren will und über Ausnahmen nach den konkreten Umständen entscheidet.<sup>597</sup> Dieser Ansicht hält GLARNER m.E. zu Recht entgegen, dass der Zweck einer Zugangsschranke immer im Ausschluss von unberechtigten Personen besteht, und zwar ungeachtet der Erfordernisse, die erfüllt sein müssen, um eine Zugangsberechtigung zu erhalten. Aus diesem Blickwinkel kann es keine Rolle spielen, ob die Daten gegen Entgelt allgemein zugänglich sind oder ob der Werkzugang aufgrund anderer als finanzieller Kriterien gewährt wird.<sup>598</sup>

---

<sup>593</sup> WEISSENBERGER, BSK StGB II, Art. 143 N 1; DONATSCH, Strafrecht III, 195; TRECHSEL/CRAMERI, PK StGB, Art. 143 N 1; GLARNER, Musikpiraterie im Internet, 168.

<sup>594</sup> WEISSENBERGER, BSK StGB II, Art. 143 N 6 ff.; TRECHSEL/CRAMERI, PK StGB, Art. 143 N 3; STRATENWERTH/JENNY/BOMMER, § 14 N 24 f.; SCHWARZENEGGER, FS-Trechsel, 313.

<sup>595</sup> WEISSENBERGER, BSK StGB II, Art. 143 N 18 ff.; DONATSCH, Strafrecht III, 196; TRECHSEL/CRAMERI, PK StGB, Art. 143 N 5; STRATENWERTH/JENNY/BOMMER, § 14 N 29.

<sup>596</sup> BALTISSER, 63; WEISSENBERGER, BSK StGB II, Art. 143 N 18 ff.; DONATSCH, Strafrecht III, 196; TRECHSEL/CRAMERI, PK StGB, Art. 143 N 6; STRATENWERTH/WOHLERS, Art. 143 N 2; STRATENWERTH/JENNY/BOMMER, § 14 N 29.

<sup>597</sup> STRATENWERTH/JENNY/BOMMER, § 14 N 30; gl. M. WEISSENBERGER, BSK StGB II, Art. 143 N 22; TRECHSEL/CRAMERI, PK StGB, Art. 143 N 6; STRATENWERTH/WOHLERS, Art. 143 N 2; HURTADO POZO, PS, N 1039.

<sup>598</sup> Vgl. GLARNER, Musikpiraterie im Internet, 171.



Beim Tatbestandsmerkmal der „Beschaffung“ ist umstritten, ob bereits die 246  
blosse Wahrnehmung bzw. Kenntnissnahme ausreichend ist, oder ob darüber  
hinaus eine eigene Verfügungsgewalt begründet werden muss. Gewisse Au-  
toren lassen bereits die blosse Kenntnissnahme genügen, während von einem  
anderen Teil der Lehre gefordert wird, dass sich der Täter – in Analogie zum  
Diebstahl – eine gewahrsamsähnliche Stellung verschaffen muss.<sup>599</sup>  
DONATSCH hält eine Analogie zum Diebstahl für verfehlt, da an Daten, an-  
ders als etwa bei körperlichen Gegenständen, keine gewahrsamsähnliche  
Stellung erlangt werden muss, damit der Täter diese für seine Zwecke nutzen  
kann.<sup>600</sup> Falls ein Täter auf ein Firmennetzwerk unter Umgehung von Zu-  
gangssperren zugreift und aus den dort abgespeicherten Dokumenten, bör-  
senkursrelevante Daten entnimmt, reicht dies bereits aus, um mit den Daten  
arbeiten zu können. Gleiches gilt auch für den Konsum urheberrechtlich  
geschützter Werke. Damit ein Nutzer unter Umgehung eines passwortgesi-  
icherten Zugangs kostenpflichtige Inhalte eines Streaming-Dienstes konsu-  
mieren kann, ist keine gewahrsamsähnliche Stellung an den Daten vorausge-  
setzt. Zur Befriedigung des Konsums reicht es aus, dass der Täter zu einem  
bestimmten Zeitpunkt während der Wiedergabe über die Daten verfügen und  
diese mittels entsprechender Software für die menschlichen Sinne wahr-  
nehmbar machen kann. Deshalb muss m.E. bereits die blosse Kenntnissnah-  
me der geschützten Daten ausreichen, um den Tatbestand von Art. 143 StGB  
zu erfüllen.<sup>601</sup> Die Umgehung einer Zugangsschranke zum Zwecke des un-  
rechtmässigen Abrufs geschützter kostenpflichtiger Daten erfüllt somit den  
Tatbestand der unbefugten Datenbeschaffung gemäss Art. 143 StGB. Der  
Täter, welcher eine Zugangsschranke zu kostenpflichtigen Angeboten um-  
geht, handelt mit der Absicht der Ersparnisbereicherung, weshalb auch das  
subjektive Tatbestandsmerkmal der Bereicherungsabsicht erfüllt ist.<sup>602</sup>

---

<sup>599</sup> Blosse Kenntnissnahme der Daten genügt; vgl. WEISSENBERGER, BSK StGB II, Art. 143 N 26; DONATSCH, Strafrecht III, 196; CORBOZ, Art. 143 N 9; STRATENWERTH/JENNY/BOMMER, § 14 N 31; a.A. TRECHSEL/CRAMERI, PK StGB, Art. 143 N 7; HURTADO POZO, PS, N 1042 und SCHMID, § 4 N 54, die eine gewahrsamsähnliche Stellung fordern.

<sup>600</sup> DONATSCH, Strafrecht III, 197.

<sup>601</sup> Gl. M. WEISSENBERGER, BSK StGB II, Art. 143 N 26; DONATSCH, Strafrecht III, 197; Botschaft Cyberkriminalität, 4705.

<sup>602</sup> BGE 129 III 646, Erw. 4.2, eine sog. Ersparnisbereicherung beruht entweder auf einer Nichtverminderung der Aktiven oder einer Nichterhöhung der Passiven.

**b)      *Unbefugtes Eindringen in ein Datenverarbeitungssystem*  
(Art. 143<sup>bis</sup> StGB)**

247 Der Tatbestand von Art. 143<sup>bis</sup> Abs. 1 StGB soll Datenverarbeitungsanlagen vor unberechtigten Eindringlingen, sog. Hackern, schützen.<sup>603</sup> Der objektive Tatbestand ist erfüllt, wenn der Täter unbefugterweise auf dem Wege von Datenübertragungseinrichtungen in ein fremdes, gegen den unbefugten Zugriff besonders gesichertes Datenverarbeitungssystem eindringt.<sup>604</sup> Der Begriff der Fremdheit ist nicht in einem sachenrechtlichen Sinne zu verstehen, sondern es ist dabei vielmehr auf die fehlende Zugangsberechtigung zum System abzustellen.<sup>605</sup> Gleiches soll gelten, wenn der Täter zu einzelnen Systemteilen keine Zugangsberechtigung hat.<sup>606</sup> Wie Art. 143 StGB fordert auch Art. 143<sup>bis</sup> StGB, dass die Datenverarbeitungssysteme durch Passwörter oder andere Zugangsschranken besonders gesichert sind.<sup>607</sup> Der subjektive Tatbestand von Art. 143<sup>bis</sup> aStGB setzte bis zur Umsetzung des Bundesbeschlusses über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. März 2011 neben dem Vorsatz das Fehlen einer Bereicherungsabsicht voraus.<sup>608</sup> Handelte der Täter, der in ein Computersystem eindrang, mit Bereicherungsabsicht, konnte er nicht nach Art. 143<sup>bis</sup> aStGB bestraft werden.<sup>609</sup> Mit dem erwähnten Bundesbeschluss wurde das subjektive Tatbestandsmerkmal der fehlenden Bereicherungsabsicht gestrichen. Seit dem 1. Januar 2012 umfasst der Anwendungs-

---

<sup>603</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 4; DONATSCH, Strafrecht III, 199 f.; TRECHSEL/CRAMERI, PK StGB, Art. 143<sup>bis</sup> N 1; STRATENWERTH/WOHLERS, Art. 143 N 1; STRATENWERTH/JENNY/BOMMER, § 14 N 37; SCHMID, § 5 N 11; Botschaft StGB 1991, 1011.

<sup>604</sup> Urteil 6B.615/2014 des Bundesgerichts vom 2. Dezember 2014, Erw. 4.3; WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 8 ff.; DONATSCH, Strafrecht III, 200 f.; TRECHSEL/CRAMERI, PK StGB, Art. 143<sup>bis</sup> N 6 ff.; HURTADO POZO, PS, N 1065.

<sup>605</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 11 ff.; DONATSCH, Strafrecht III, 200; STRATENWERTH/WOHLERS, Art. 143<sup>bis</sup> N 1; CORBOZ, Art. 143<sup>bis</sup> N 2; HURTADO POZO, PS, N 1061; a.A. SCHMID, § 5 N 17.

<sup>606</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 12; STRATENWERTH/WOHLERS, Art. 143<sup>bis</sup> N 1; TRECHSEL/CRAMERI, PK StGB, Art. 143<sup>bis</sup> N 4; a.A. STRATENWERTH/JENNY/BOMMER, § 14 N 39.

<sup>607</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 14 ff.; STRATENWERTH/WOHLERS, Art. 143<sup>bis</sup> N 1; TRECHSEL/CRAMERI, PK StGB, Art. 143<sup>bis</sup> N 5.

<sup>608</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 27; DONATSCH, Strafrecht III, 202; Bundesbeschluss Cyberkriminalität, 2767.

<sup>609</sup> STRATENWERTH/JENNY/BOMMER, § 14 N 39; SCHWARZENEGGER, ZSR 2008 II, 494; GLARNER, Musikpiraterie im Internet, 174.

bereich von Art. 143<sup>bis</sup> Abs. 1 StGB somit auch Taten mit Bereicherungsabsicht.<sup>610</sup> Das Risiko einer Strafbarkeitslücke von Art. 143<sup>bis</sup> aStGB wurde damit ausgeräumt.<sup>611</sup> Zudem wurde Art. 143<sup>bis</sup> StGB um einen Abs. 2 mit folgendem Wortlaut erweitert: „Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit einer Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft“. Dadurch werden die Vorbereitungshandlungen zum „Hacking“ unter Strafe gestellt.<sup>612</sup>

Die kostenpflichtigen Streaming-Dienste verwenden spezielle Software, um die angebotenen Werke vor unbefugtem Zugriff zu schützen. Das Zusammenspiel aus Software und Hardware ist als Datenverarbeitungssystem i.S.v. Art. 143<sup>bis</sup> StGB zu qualifizieren.<sup>613</sup> Der unbefugte Zugriff auf passwortgesicherte Inhalte eines Streaming-Dienstes stellt ein unbefugtes Eindringen in ein Datenverarbeitungssystem i.S.v. Art. 143<sup>bis</sup> StGB dar.<sup>614</sup>

**c) *Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)***

Der Straftatbestand von Art. 147 StGB schützt das Vermögen und ist dem Betrug nach Art. 146 StGB weitgehend nachgebildet.<sup>615</sup> Ein Betrug liegt jedoch nur vor, wenn ein Mensch getäuscht wurde.<sup>616</sup> Art. 147 StGB modifiziert den Betrugstatbestand dahingehend, dass er auf Fälle anwendbar ist, in denen nicht ein Mensch getäuscht, sondern eine Datenverarbeitungsanlage

---

<sup>610</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 27; DONATSCH, Strafrecht III, 202.

<sup>611</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 27; DONATSCH, Strafrecht III, 202; Botschaft Cyberkriminalität, 4703 f., dadurch sollen die Vorbereitungshandlungen zum *Hacking* unter Strafe gestellt werden.

<sup>612</sup> Vgl. WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 34 ff.; DONATSCH, Strafrecht III, 202 f.

<sup>613</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 9; PFISTER, 57 ff.; SCHMID, § 5 N 16.

<sup>614</sup> Dies gilt unabhängig davon, ob es sich um sog. Flatrate oder Pay-per-View Angebote handelt.

<sup>615</sup> FIOLKA, BSK StGB II, Art. 147 N 6; DONATSCH, Strafrecht III, 248; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 1 StGB; STRATENWERTH/JENNY/BOMMER, § 16 N 2; BGE 129 IV 22, Erw. 4.2.; a.A. SCHMID, § 7 N 14.

<sup>616</sup> DONATSCH, Strafrecht III, 248; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 1; STRATENWERTH/WOHLERS, Art. 147 N 1; BGE 129 IV 315, Erw. 2.1.

manipuliert wird.<sup>617</sup> Der objektive Tatbestand setzt voraus, dass der Täter auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Übermittlungsvorgang einwirkt.<sup>618</sup> Zunächst werden Fälle erfasst, in denen unrichtige Daten, d.h. Daten, die mit der tatsächlichen Sach- und Rechtslage nicht übereinstimmen, verwendet werden.<sup>619</sup> Die Variante der unvollständigen Verwendung von Daten stellt einen Unterfall der unrichtigen Verwendung von Daten dar.<sup>620</sup> Dabei werden gewisse Daten pflichtwidrig nicht bzw. an sich richtige Daten nur lückenhaft eingegeben.<sup>621</sup> Die Variante der unbefugten Verwendung von Daten umfasst Konstellationen, in denen unbefugte Personen „durch die an sich «richtige» Verwendung von Daten in die Datenverarbeitung eingreifen“<sup>622</sup>.<sup>623</sup> Schliesslich soll die Formulierung „in vergleichbarer Weise“ ermöglichen, „auch Manipulationen zu erfassen“, die nicht ohne Weiteres unter die vorstehend erwähnten Datenmanipulationen fallen.<sup>624</sup> Da auch solche Eingriffe jeweils als unrichtige Verwendung qualifiziert werden können, kommt dieser Tatbestandsvariante im Ergebnis keine eigenständige Bedeutung zu.<sup>625</sup>

- 250 Der objektive Tatbestand setzt zudem voraus, dass der Täter eine Vermögensverschiebung zum Schaden eines anderen herbeiführt oder eine solche unmittelbar danach verdeckt. Eine Vermögensverschiebung i.S.v. Art. 147 StGB ist auch dann zu bejahen, wenn eine Übertragung unterlassen wird,

---

<sup>617</sup> DONATSCH, Strafrecht III, 249 f.; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 1 f.; STRATENWERTH/JENNY/BOMMER, § 16 N 2; Botschaft StGB 1991, 1020.

<sup>618</sup> FIOLKA, BSK StGB II, Art. 147 N 9 ff.; DONATSCH, Strafrecht III, 249 f.; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 4 ff.; STRATENWERTH/WOHLERS, Art. 147 N 3.

<sup>619</sup> FIOLKA, BSK StGB II, Art. 147 N 9; DONATSCH, Strafrecht III, 249; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 4.

<sup>620</sup> FIOLKA, BSK StGB II, Art. 147 N 10; DONATSCH, Strafrecht III, 249; HURTADO POZO, PS, N 1053; SCHMID, § 7 Rn. 54.

<sup>621</sup> FIOLKA, BSK StGB II, Art. 147 N 10; DONATSCH, Strafrecht III, 249; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 5; STRATENWERTH/JENNY/BOMMER, § 16 N 6; HURTADO POZO, PS, N 1237; Botschaft StGB 1991, 1021.

<sup>622</sup> Botschaft StGB 1991, 1021.

<sup>623</sup> Vgl. FIOLKA, BSK StGB II, Art. 147 N 11; DONATSCH, Strafrecht III, 249; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 6; STRATENWERTH/JENNY/BOMMER, § 16 N 7; Botschaft StGB 1991, 1021.

<sup>624</sup> FIOLKA, BSK StGB II, Art. 147 N 18; DONATSCH, Strafrecht III, 250; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 6; STRATENWERTH/JENNY/BOMMER, § 16 N 9; CORBOZ, Art. 147 N 7 StGB; HURTADO POZO, PS, N 1244; SCHMID, § 7 N 77 ff.

<sup>625</sup> FIOLKA, BSK StGB II, Art. 147 N 18, sieht in dieser Tatbestandsvariante eine „reine Angst- und Absicherungsklausel“, die sich mit dem Bestimmtheitsgebot nur schwer vereinbaren lässt.

obschon eine Rechtspflicht eine solche gefordert hätte.<sup>626</sup> Beim subjektiven Tatbestand wird kumulativ zum Vorsatz die Absicht des Täters gefordert, sich oder einen anderen zu bereichern.<sup>627</sup>

Bei kostenpflichtigen Streaming-Diensten wird der Zugriff auf die geschütz- 251  
ten Inhalte nur gegen Entrichtung eines Entgelts (*pay-per-view* oder *flatrate*)  
gewährt. Falls der Täter unter Umgehung einer Zugangsschranke urheber-  
rechtlich geschützte Werke verwendet, liegt bei diesem eine Ersparnisberei-  
cherung vor.

Gemäss SCHMID muss – dem Betrugstatbestand folgend – bei Art. 147 StGB 252  
der zu verschiebende Vermögenswert verschieden von demjenigen sein, der  
in der Datenverarbeitung selbst und im Gegenwert ihrer Benutzung liegt.<sup>628</sup>  
Bei der Nutzung eines Streaming-Portals liegt die charakteristische Leistung  
nicht im Erwerb eines digitalen Werks, sondern erschöpft sich vielmehr im  
blossenen Konsum desselben unter Nutzung der kostenpflichtigen Infrastruktur  
des Anbieters. Dabei steht – vergleichbar mit der Situation bei einem Kino-  
besuch – der Werkgenuss im Vordergrund. Erschlichen wird die Nutzung der  
Infrastruktur des Stream-Anbieters. Deshalb lässt sich die Umgehung von  
Zugangsschranken zum Zweck des Streaming von kostenpflichtigen ge-  
schützten Werken, nicht unter den Tatbestand von Art. 147 StGB subsumie-  
ren.

#### **d) Erschleichen einer Leistung (Art. 150 StGB)**

##### **aa) Allgemeines**

Durch Art. 150 StGB wird das Erschleichen einer Leistung ohne Bezahlung 253  
unter Strafe gestellt. Schutzobjekt dieser als Auffangtatbestand zu Art. 146  
StGB konzipierten Bestimmung ist das Vermögen.<sup>629</sup> Strafrechtlich erfasst  
werden betrugsähnliche Verhaltensweisen, in denen ohne motivierende Ein-  
wirkung auf andere, ohne individuelle Vermögensdisposition oder konkret  
nachzuweisende Schädigung des Leistenden eine geldwerte Leistung er-

---

<sup>626</sup> TRECHSEL/CRAMERI, PK StGB, Art. 147 N 9.

<sup>627</sup> FIOLKA, BSK StGB II, Art. 147 N 40; DONATSCH, Strafrecht III, 252; STRATENWERTH/  
WOHLERS, Art. 147 N 5.

<sup>628</sup> SCHMID, § 7 N 93.

<sup>629</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 1; TRECHSEL/CRAMERI, PK StGB, Art. 150  
N 1; STRATENWERTH/WOHLERS, Art. 150 N 1.

schlichen wird.<sup>630</sup> Ein Vermögensschaden muss nicht nachgewiesen werden, da es sich bei Art. 150 StGB um ein als „Begehungsdelikt konzipiertes schlichtes Tätigkeitsdelikt“<sup>631</sup> handelt. Bei der Teilrevision 1994 wurde neu das Erschleichen einer Leistung, die von einer Datenverarbeitungsanlage erbracht wird, der sog. Zeitdiebstahl, in den Tatbestand aufgenommen.<sup>632</sup> Unter Zeitdiebstahl versteht man die unrechtmässige Nutzung von Rechenleistung fremder Computeranlagen für eigene Zwecke.

*bb) Erschleichen*

- 254 Erschleichen bedeutet „Erlangen durch unlauteres Verhalten“ und beinhaltet eine gewisse Heimlichkeit.<sup>633</sup> Damit der Tatbestand erfüllt ist, muss das Vorgehen, mit dem der Täter technische oder menschliche Sicherheitsvorkehrungen gegen die unerlaubte Benutzung umgeht, als heimlich oder täuschend zu qualifizieren sein.<sup>634</sup> Als Beispiel wird etwa die Verwendung von Hackerprogrammen zur Erlangung des Zugangs zu Leistungen aufgeführt.<sup>635</sup>

*cc) Leistung*

- 255 Betreffend die Tragweite des Leistungsbegriffs werden in der Lehre unterschiedliche Auffassungen vertreten.<sup>636</sup> Die wohl herrschende Meinung spricht sich für eine enge Auslegung des Wortlautes aus und will lediglich Dienstleistungen unter den Tatbestand von Art. 150 StGB subsumieren.<sup>637</sup>

---

<sup>630</sup> TRECHSEL/CRAMERI, PK StGB, Art. 150 N 1; STRATENWERTH/JENNY/BOMMER, § 16 N 49.

<sup>631</sup> SCHMID, § 9 N 13.

<sup>632</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 2; TRECHSEL/CRAMERI, PK StGB, Art. 150 N 2; Botschaft StGB 1991, 1030 ff.

<sup>633</sup> TRECHSEL/CRAMERI, PK StGB, Art. 150 N 2 StGB; STRATENWERTH/WOHLERS, Art. 150 N 2; BGE 117 IV 449, Erw. 6.a; BGE 104 Ia 88, Erw. 12.a.

<sup>634</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 9; TRECHSEL/CRAMERI, PK StGB, Art. 150 N 4; STRATENWERTH/JENNY/BOMMER, § 16 N 50.

<sup>635</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 24; DONATSCH, Strafrecht III, 265; TRECHSEL/CRAMERI, PK StGB, Art. 150 N 4; STRATENWERTH/JENNY/BOMMER, § 16 N 50.

<sup>636</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 23 ff.; DONATSCH, Strafrecht III, 265; TRECHSEL/CRAMERI, PK StGB, Art. 150 N 5 ff.; STRATENWERTH/WOHLERS, Art. 150 N 1; CORBOZ, Art. 150 N 24.

<sup>637</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 4 und N 23, wonach auch „Konstellationen, in denen der Zugang zu Datenbanken gegen Bezahlung angeboten wird“, erfasst seien; TRECHSEL/CRAMERI, PK StGB, Art. 150 N 3; STRATENWERTH/JENNY/BOMMER, § 16 N 53.

Andere Autoren wollen auch Sachleistungen (z.B. die Inanspruchnahme eines Warenautomaten) vom Tatbestand her nicht ausschliessen, mit der Begründung, dass es sich bei dieser Konstellation vielmehr um ein Konkurrenzproblem handeln würde.<sup>638</sup> Ein Teil der Lehre geht deshalb von einem weit gefassten Leistungsbegriff aus, der auch Sachleistungen mitumfasst.<sup>639</sup>

Der *Download* von kostenpflichtigen geschützten Werken ist nicht als (digitale) Dienstleistung, sondern als digitale Sachleistung zu qualifizieren, da hier nicht die Nutzung von Rechenleistung eines Computers oder die Übertragungskapazitäten eines Netzwerks im Vordergrund stehen, sondern die Erlangung eines immateriellen Gutes, das nach erfolgter Übermittlung dauerhaft beim Leistungsempfänger verbleibt.<sup>640</sup> 256

Im Unterschied dazu verbleibt beim Streaming i.d.R. keine dauerhafte Kopie des Werks auf dem Rechner des Empfängers. Die charakteristische Leistung liegt nicht in der Erlangung eines digitalen Werks sondern vielmehr in der Nutzung des Streaming-Dienstes, der es seinen Nutzern ermöglicht – unter Verwendung von dessen Software und *Server-Infrastruktur* – geschützte Inhalte mittels Streaming-Verfahren zu konsumieren. Folglich wird bei der Umgehung von Zugangsschranken zum Zweck des Konsums kostenpflichtiger geschützter Werke mittels Streaming-Verfahren eine Dienstleistung erschlichen. 257

#### dd) *Entgeltlichkeitserfordernis*

Eine Leistung gilt dann als entgeltlich, wenn sie nur im Austausch für eine vermögenswerte Gegenleistung erbracht wird.<sup>641</sup> Nach Ansicht von SCHMID lässt die grammatikalische Interpretation des Wortlauts von Art. 150 StGB keine weitergehende Auslegung zu, als dass die Bestimmung einzig auf Leistungen Anwendung findet, die gegen Entgelt angeboten werden.<sup>642</sup> Wird der Zugang zu einem Streaming-Dienst durch technische Massnahmen gesichert und einzig gegen Bezahlung eines Entgelts gewährt, ist das Kriterium der 258

---

<sup>638</sup> STRATENWERTH/WOHLERS, Art. 150 N 1 und N 4, wonach Art. 150 StGB verdrängt wird, wenn der Täter durch sein Verhalten die Straftatbestände nach Art. 139, 146 und 147 StGB erfüllt.

<sup>639</sup> STRATENWERTH/WOHLERS, Art. 150 N 1; RUBLI, Rz. 208; BGE 104 IV 72, Erw. 1.c.

<sup>640</sup> SCHWARZENEGGER, ZSR 2008 II, 497 f.; LUXEM, 20; a.A. GLARNER, Musikpiraterie im Internet, 178, der das Anbieten geschützter Inhalte zum *Download* als Dienstleistung qualifiziert.

<sup>641</sup> STRATENWERTH/WOHLERS, Art. 150 N 1; STRATENWERTH/JENNY/BOMMER, § 16 N 50.

<sup>642</sup> SCHMID, § 9 N 22.

Entgeltlichkeit erfüllt. Letztlich wird mit dem Einsatz von Zugangsschranken gerade der Zweck verfolgt, die monetären Interessen der Rechteinhaber gegenüber den Nutzern durchzusetzen.

*ee) Öffentlichkeitserfordernis*

- 259 Ein Teil der Lehre vertritt die Meinung, dass nur solche Leistungen von Art. 150 StGB umfasst sind, die öffentlich einem grösseren Kreis von Personen gegen Entgelt angeboten werden.<sup>643</sup> Das Tatbestandsmerkmal der Öffentlichkeit des Angebots wird aus der verlangten Öffentlichkeit des Verkehrsmittels und dem Wesen von Aufführungen und aufgestellten Automaten hergeleitet und auf den Grundtatbestand übertragen.<sup>644</sup> Gegen das Kriterium der Öffentlichkeit der Leistung wird vorgebracht, dieses sei deshalb eingeführt worden, weil unpersönliche Leistungsträger (Automaten) im Zeitpunkt, als diese Norm geschaffen worden war, vorwiegend im öffentlichen Raum anzutreffen waren.<sup>645</sup> Das Öffentlichkeitserfordernis ist in die Generalklausel nicht aufgenommen worden, damit durch extensive Auslegung des Wortlauts auch zukünftige, durch den technischen Fortschritt bedingte Betrügereien erfasst werden können.<sup>646</sup>
- 260 Da sämtliche Angebote von Streaming-Diensten ohnehin an die breite Öffentlichkeit gerichtet sind, kann diese Frage vorliegend offengelassen werden. Die Nutzung kostenpflichtiger Streaming-Dienste steht – gegen Bezahlung einer entsprechenden Nutzungsgebühr – grundsätzlich jedermann offen.<sup>647</sup>

*ff) Vorsatz*

- 261 Damit der subjektive Tatbestand erfüllt ist, muss der Täter vorsätzlich handeln.<sup>648</sup> Eine Bereicherungsabsicht ist bei Art. 150 StGB nicht erforder-

---

<sup>643</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 5 und N 23; DONATSCH, Strafrecht III, 265; TRECHSEL/CRAMERI, PK StGB, Art. 150 N 3.

<sup>644</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 4 f. und N 25; HURTADO POZO, PS, N 1318.

<sup>645</sup> RUBLI, Rz. 210, m.w.H.

<sup>646</sup> RUBLI, Rz. 210.

<sup>647</sup> Ausnahmen dazu bilden bspw. territoriale Schranken, falls das Sendegebiet durch den Einsatz von Geo-Sperren auf einzelne Staaten beschränkt werden soll. Aber auch hier gilt, dass innerhalb des jeweiligen Sendegebietes sämtlichen (zahlenden) Nutzern Zugriff auf die Datenangebote gewährt wird.

<sup>648</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 28 f., ist der Ansicht, dass ein eventualvorsätzliches Handeln nur schwer vorstellbar sei, da der Täter „nach dem klaren Gesetzes-



lich.<sup>649</sup> Ebenso ist unerheblich, ob der Täter die Leistung für sich oder einen anderen will.<sup>650</sup>

Bei kostenpflichtigen Streaming-Diensten, die den Zugang zu den angebotenen Werken durch wirksame technische Massnahmen sichern, ist es für die Nutzer unstreitig erkennbar, dass der Werkzugriff nur gegen Entrichtung eines Entgelts eingeräumt wird (flatrate, pay-per-view etc.). Daher ist bei der Umgehung passwortgesicherter Zugangsschranken zu kostenpflichtigen Streaming-Diensten ein vorsätzliches Handeln zu bejahen. 262

**e) Konkurrenzen der computerstrafrechtlichen Bestimmungen**

Gemäss einem Teil der Lehre ist Art. 150 StGB subsidiär zu Art. 143 StGB.<sup>651</sup> Gewisse Autoren plädieren dafür, dass Art. 150 StGB gegenüber Art. 143 StGB in jenen Fällen vorgehen soll, in denen der Täter Zugangssicherungen überwindet, die ein Datenangebot schützen, welches für jedermann gegen Entgelt zugänglich ist.<sup>652</sup> Nach hier vertretener Ansicht ist von echter Konkurrenz auszugehen, da Art. 150 StGB primär den Schutz des Vermögens der Leistungserbringer bezweckt, während Art. 143 StGB das Verfügungsrecht über Computerdaten schützt.<sup>653</sup> 263

---

wortlaut um die Entgeltlichkeit der konkreten Leistung *wissen* und das Entgelt bewusst nicht oder nicht voll entrichten [will]“; DONATSCH, Strafrecht III, 267; STRATENWERTH/WOHLERS, Art. 150 N 3; STRATENWERTH/JENNY/BOMMER, § 16 N 51, sehen den Eventualvorsatz nicht ausgeschlossen; ebenso CORBOZ, Art. 150 N 32 f. und HURTADO POZO, PS, N 1327.

<sup>649</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 30; DONATSCH, Strafrecht III, 267; STRATENWERTH/JENNY/BOMMER, § 16 N 51; CORBOZ, Art. 150 N 33; HURTADO POZO, PS, N 1327.

<sup>650</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 30; CORBOZ, Art. 150 N 7.

<sup>651</sup> TRECHSEL/CRAMERI, PK StGB, Art. 150 N 9; DONATSCH, Strafrecht III, 269, wonach Art. 150 StGB durch Art. 143 StGB konsumiert wird; STRATENWERTH/WOHLERS, Art. 150 N 4; HURTADO POZO, PS, N 1333; GLARNER, Musikpiraterie im Internet, 179; Botschaft StGB 1991, 1031.

<sup>652</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 41; STRATENWERTH/JENNY/BOMMER, § 16 N 54; MOREILLON, medialex 2001, 22.

<sup>653</sup> Ebenso CORBOZ, Art. 150 N 41.

- 264 Der als reines Verletzungsdelikt konzipierte Art. 150 StGB konsumiert Art. 143<sup>bis</sup> StGB, der Aspekte eines Vermögensgefährdungsdelikts aufweist.<sup>654</sup>
- 265 Grundsätzlich geht Art. 147 StGB dem Tatbestand von Art. 150 StGB vor, da bei erstgenannter Bestimmung eine Einwirkung auf eine Datenverarbeitungsanlage verlangt wird, welche über das weit gefasste Tatbestandsmerkmal der Erschleichung hinausgeht.<sup>655</sup> Bei einem reinen Zeit- oder Leistungsdiebstahl geht Art. 150 StGB ausnahmsweise vor, solange die in Anspruch genommene Leistung nicht einem anderen berechnet wird.<sup>656</sup>
- 266 Da Art. 143 StGB die Überwindung einer besonderen Zugriffssicherung verlangt, geht diese – nach Ansicht von RUBLI – als speziellere Norm gegenüber der Bestimmung von Art. 147 StGB vor, die lediglich eine Einwirkung auf eine Datenverarbeitungsanlage voraussetzt.<sup>657</sup> M.E. ist auch hier von echter Konkurrenz auszugehen, weil das geschützte Rechtsgut bei Art. 147 StGB das Vermögen darstellt, während Art. 143 StGB das Verfügungsrecht über Computerdaten schützt.<sup>658</sup>
- 267 Zwischen Art. 147 und Art. 143<sup>bis</sup> StGB besteht echte Konkurrenz, da verschiedene Rechtsgüter betroffen sind und beim Computerbetrug nicht zwingend ein Eindringen in eine Datenverarbeitungsanlage zur Erfüllung des Tatbestandes vorausgesetzt ist.<sup>659</sup>

---

<sup>654</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 31 und Art. 150 N 42; DONATSCH, Strafrecht III, 269; TRECHSEL/CRAMERI, PK StGB, Art. 143<sup>bis</sup> N 12 und Art. 150 N 9; STRATENWERTH/JENNY/BOMMER, § 16 N 54; CORBOZ, Art. 150 N 41; HURTADO POZO, PS, N 1333; a.A. SCHMID, § 5 Rn. 40, der für echte Konkurrenz postuliert.

<sup>655</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 44; DONATSCH, Strafrecht III, 202, 268; STRATENWERTH/WOHLERS, Art. 150 N 4; RUBLI, Rz. 541; SCHMID, § 9 Rn. 47 f.; a.A. FIOKA, BSK StGB II, Art. 147 N 56.

<sup>656</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 44; TRECHSEL/CRAMERI, PK StGB, Art. 150 N 9; STRATENWERTH/JENNY/BOMMER, § 16 N 54; SCHMID, § 9 Rn. 47 ff.; abweichend Botschaft StGB 1991, 1032; teilweise abweichend CORBOZ, Art. 150 N 40 und HURTADO POZO, PS, N 1333.

<sup>657</sup> RUBLI, Rz. 541.

<sup>658</sup> Vgl. dazu FIOKA, BSK StGB II, Art. 147 N 47, der von einer echten Konkurrenz ausgeht, „wenn die unbefugt beschafften Daten selber einen ökonomischen Wert darstellen“; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 16.

<sup>659</sup> FIOKA, BSK StGB II, Art. 147 N 48; a.A. TRECHSEL/CRAMERI, PK StGB, Art. 147 N 16, wonach Art. 143<sup>bis</sup> StGB gegenüber sämtlichen übrigen Computerdelikten subsidiär ist; ebenso HURTADO POZO, PS, N 1074 und SCHMID, § 5 Rn. 38.

Dringt der Täter unrechtmässig und mit Bereicherungsabsicht in eine Daten- 268  
verarbeitungsanlage ein und verfügt sodann über geschützte Daten, wird  
Art. 143<sup>bis</sup> von Art. 143 StGB konsumiert.<sup>660</sup>

## 7. Umgehung von Geo-Sperren<sup>661</sup>

Aus unterschiedlichen Motiven wollen Streaming-Dienste verhindern, dass 269  
Nutzer von ausserhalb eines bestimmten Territoriums Zugang zu ihren An-  
geboten erhalten.<sup>662</sup> Oftmals haben die Lizenznehmer nur die Verwertungs-  
rechte für ein bestimmtes geografisches Gebiet (z.B. USA und Kanada) er-  
worben, weshalb die kommerzielle Verwertung der entsprechenden Werke  
auf diese Gebiete beschränkt bleibt.<sup>663</sup> Sodann eröffnen Geo-Sperren den  
Streaming-Diensten die Möglichkeit, die Auswahl der Inhalte länderspezi-  
fisch anzupassen und zu unterschiedlichen Konditionen anzubieten.<sup>664</sup>

### A. Technische Einführung

Der Zugriff zum Internet wird über eine weltweit einmalig vergebene IP- 270  
Adresse hergestellt.<sup>665</sup> In der Regel erhalten die Internetnutzer bei jeder Ein-  
wahl eine neue IP-Adresse von ihrem Zugangsanbieter (z.B. UPC Cablecom,  
Swisscom, Sunrise etc.). Die genaue Adresse, die der einzelne Nutzer erhält,  
bestimmt sich nach einem streng hierarchisch gegliederten System, an deren  
Spitze die *Internet Assigned Numbers Authority* (IANA<sup>666</sup>) steht, welche  
weltweit fünf verschiedenen *Regional Internet Registries* (RIRs) die IP-

---

<sup>660</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 30; DONATSCH, Strafrecht III, 202;  
TRECHSEL/CRAMER, PK StGB, Art. 143<sup>bis</sup> N 12; HURTADO POZO, PS, N 1074; SCHMID,  
§ 5 Rn. 34 ff.; Botschaft Cyberkriminalität, 4704.

<sup>661</sup> Zur Terminologie vgl. PRILL, Fn. 181.

<sup>662</sup> HILGERT/GRETH, 115; PRILL, 36; REINBACHER, HFR 2012, 179; MITSDÖRFFER/  
GUTFLEISCH, MMR 2009, 731; HOEREN, MMR 2007, 3 f.

<sup>663</sup> REINBACHER, HFR 2012, 179.

<sup>664</sup> So kostet bspw. ein Spotify-Premium-Abonnement in der Schweiz monatlich mehr als  
das Doppelte gegenüber der Gebühr, welche die Nutzer in Polen bezahlen müssen.

<sup>665</sup> SCHEDER-BIESCHIN, 63; REINBACHER, HFR 2012, 179; MITSDÖRFFER/GUTFLEISCH,  
MMR 2009, 731.

<sup>666</sup> Die IANA ist eine Abteilung der ICANN; <<https://iana.org>> (besucht 25. August 2015);  
zur ICANN vgl. auch WEIGELE, MMR 2013, 17 ff. und GASSER/BURKERT/THOUVENIN/  
NOLAN, 470 ff., m.w.H.; VOEGELI-WENZL, GRUR-Int. 2007, 808 ff.; BECHTOLD, Infor-  
mationsrecht, 442.

3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers

---

Adressräume zuteilt.<sup>667</sup> Die regionalen Vergabestellen (RIRs) wiederum vergeben bestimmte Bereiche aus den ihnen zugeteilten Adressräumen an lokale Vergabestellen (*Local Internet Registries*; LIRs), wie etwa *Access-Provider*, Grossunternehmen und öffentliche Einrichtungen.<sup>668</sup> Diese wiederum vergeben die ihnen zugewiesenen Adressräume in regional eingeteilte Blöcke weiter.<sup>669</sup> Dabei wird offengelegt, welche Adressräume an welche Stellen vergeben wurden.<sup>670</sup> Diese Informationen ermöglichen die Zuordnung einer IP-Adresse zu einem bestimmten Land.<sup>671</sup>

**a) Netzinterne Kontrollmechanismen**

- 271 Bei den netzinternen Kontrollmechanismen erfolgt die Lokalisierung des Nutzerrechners einerseits mithilfe der vom Nutzer übermittelten IP-Adresse<sup>672</sup> und andererseits durch netztopologische Informationen<sup>673</sup>. Bei der

---

<sup>667</sup> African Network Information Centre (AfriNIC), Asian Pacific Network Information Centre (APNIC), American Registry for Internet Numbers (ARIN), Latin-American and Caribbean IP Address Registry (LACNIC) und Réseaux IP Européens Network Coordination Centre (RIPE NCC); siehe auch WEBER, *digma* 2014, 95; SCHEDER-BIESCHIN, Fn. 255, PRILL, 39, m.w.H.; HENNEMANN, 246; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 731; VOEGELI-WENZL, GRUR-Int. 2007, 808; HOEREN, MMR 2007, 4.

<sup>668</sup> PRILL, 39; SCHEDER-BIESCHIN, 63; WEBER/FERCSIK SCHNYDER, *sic!* 2009, 580; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 731; HOEREN, MMR 2007, 4.

<sup>669</sup> HILGERT/GRETH, 115; SCHEDER-BIESCHIN, 63; HOEREN, MMR 2007, 4.

<sup>670</sup> SCHEDER-BIESCHIN, 63 f.; REINBACHER, HFR 2012, 179, in aller Regel wird dies auch dasjenige Land sein, in dem sich der Internetnutzer tatsächlich aufhält; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 731.

<sup>671</sup> HILGERT/GRETH, 115; REINBACHER, HFR 2012, 179; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 731.

<sup>672</sup> PRILL, 37 f., mit detaillierten Ausführungen zur Problematik der Lokalisierung eines Nutzerrechners beim Abruf einer Datei mittels „Deep-Link“. Durch Eingabe des Deep-Links kann die gewünschte Datei unter Umgehung der Startseite geladen werden. Falls die Datei nicht auf dem gleichen *Server* wie die Webseite gespeichert ist, was bei Multimediateilen oftmals der Fall ist, findet keine Lokalisierungsüberprüfung statt, wenn die Geo-Sperre in den *Web-Server* integriert ist. Die gewünschte Datei kann dann direkt vom *Streaming-Server* geladen werden. Die Anbieter können den Werkzugriff mittels Deep-Link verhindern, indem der Datei ein individueller, nur für den jeweiligen Abruf gültiger Dateiname zugeordnet wird. Wahlweise kann bei jedem einzelnen Zugriff eine sog. Session-ID mitgesendet werden. Der Zugriff auf die Datei kann diesfalls nur im Rahmen einer Sitzung erfolgen, die erst eröffnet wird, nachdem die Geo-Sperre passiert worden ist; HENNEMANN, 104; FEDERRATH, ZUM 2006, 435 ff.

<sup>673</sup> Da diese Methoden eine eher geringe praktische Nutzbarkeit aufweisen, wird auf eine eingehende Untersuchung verzichtet und auf die Ausführungen bei PRILL, 47 ff. und 110 verwiesen.

Lokalisierung mittels IP-Adresse wird beim Abruf der *URL* einer Webseite oder eines *Hyperlinks* im *Browser* ein *Access-Request* an den Betreiber der Webseite gesendet. Dieser schickt einen *Location-Request* an einen *Geolocation*-Anbieter, wobei er die IP-Adresse des Nutzers weiterleitet. Beim *Geolocation*-Anbieter findet ein Abgleich zwischen der IP-Adresse des Nutzers und den in dessen Datenbank gespeicherten Geo-Informationen statt. Anschliessend wird dem Betreiber der Webseite der vermutete Standort des Nutzers durch den Geolocation-Anbieter mitgeteilt. Gestützt auf diese Information kann der Betreiber der Webseite dem Nutzer den Zugang gewähren oder verweigern.<sup>674</sup> Durch dieses Vorgehen kann die IP-Adresse des Nutzers in über 99% der Fälle dem richtigen Staat zugeordnet werden.<sup>675</sup>

#### **b) Netzexterne Faktoren**

Nebst der IP-Adresse können auch netzexterne Faktoren wie die Spracheinstellungen oder die ausgewählte Zeitzone auf dem Nutzerrechner Aufschluss über den Aufenthaltsort des Nutzers geben.<sup>676</sup> Da diese Einstellungen aber selbst von einem wenig versierten Nutzer problemlos geändert werden können, sind diese Informationen für sich genommen nur sehr bedingt für die Lokalisierung des Nutzers geeignet. Besser wäre eine Lokalisierung mittels personenbezogener Daten wie etwa die Adressanschrift, Telefonnummer oder Kreditkarteninformationen.<sup>677</sup>

### **B. Massnahmen zur Identitätsverschleierung**

Zur Verschleierung der wahren IP-Adresse bieten sich den Nutzern verschiedene Möglichkeiten. Nachfolgend sollen die am meisten verbreiteten Techniken näher beleuchtet werden.<sup>678</sup>

#### **a) Anonymisierungsdienste**

Spezielle Anonymisierungsprogramme, wie etwa TOR oder JonDo verhindern die Übermittlung der IP-Adresse des Nutzers, indem eine Kaskade von

---

<sup>674</sup> Zum Ganzen PRILL, 40 f., m.w.H.; vgl. auch HOEREN, MMR 2007, 4.

<sup>675</sup> PRILL, 42; MITSDÖRFFER/GUTFLEISCH, MMR 2009, 732; HOEREN, ZfWG 2008, 312 f.

<sup>676</sup> PRILL, 50 f.

<sup>677</sup> PRILL, 51, weist zutreffend darauf hin, dass die Notwendigkeit einer Registrierung mit sensiblen persönlichen Daten generell eine hohe abschreckende Wirkung beinhaltet und darüber hinaus sehr kostenintensiv ist.

<sup>678</sup> PRILL, 44 ff.; HENNEMANN, 104 ff.; 246 f.

### 3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers

mindestens drei *Servern* zwischengeschaltet wird.<sup>679</sup> Jede Zwischenstation kennt dabei nur die vorhergehende und die nachfolgende Station, nicht aber das Ende der Kette. Die Kommunikation unter den (abwechselnd) hintereinander geschalteten Computern erfolgt zudem verschlüsselt. Eine direkte Kommunikation mit dem *Websserver*, auf dem die Inhalte abgespeichert sind, findet nur mit demjenigen Rechner statt, der sich am Ende dieser Kette befindet, nicht aber mit dem Computer des die Anfrage tätigen Nutzers.<sup>680</sup> Dadurch wird ein sehr hoher Grad an Anonymität gewährleistet und eine Identifizierung des Nutzers bzw. dessen Lokalisierung ist im Einzelfall praktisch unmöglich.<sup>681</sup> Zur Umgehung einer Geo-Sperre eignen sich die Anonymisierungsdienste jedoch nur bedingt, da hierbei die Datenübertragung relativ stark verlangsamt wurde und normalerweise keine *Flash*-Videos angezeigt werden konnten.<sup>682</sup> Das Problem der langsamen Datenübertragung soll durch das Projekt *High-Speed Onion Routing at the Network Layer* (HORNET) behoben werden.<sup>683</sup>

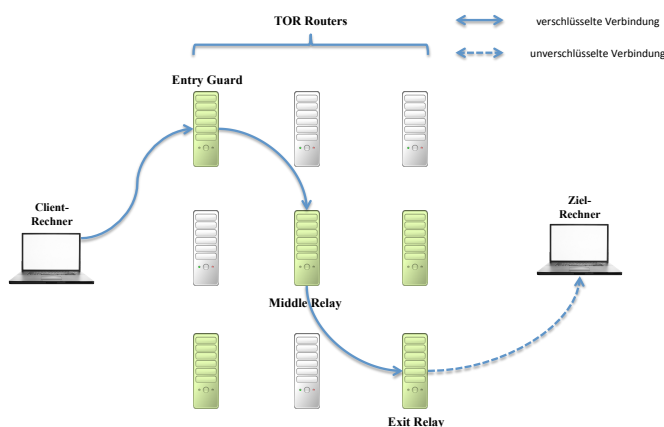


Abbildung 8: Wie TOR funktioniert, Quelle: <<https://www.torproject.org/about/overview>> (besucht 3.7.2015)

<sup>679</sup> Ausführlich dazu THIESEN, MMR 2014, 803; SCHEDER-BIESCHIN, 76 f.; REINBACHER, HFR 2012, 184.

<sup>680</sup> Vgl. PRILL, 44 f. m.w.H.; REINBACHER, HFR 2012, 184; HENNEMANN, 105.

<sup>681</sup> SCHEDER-BIESCHIN, 76 f.; REINBACHER, HFR 2012, 184; HENNEMANN, 105.

<sup>682</sup> SCHEDER-BIESCHIN, 77, weil das TOR-Netzwerk.

<sup>683</sup> STEIER, Hornet, <<http://www.nzz.ch/hornet-statt-tor-netzwerk-ld.1180>> (besucht 25. August 2015).

### b) *Proxy-Server*

Ein *Proxy-Server* ist ein Computer auf einem fremden *Server*, der Netzwerk- 275 zugriffe entgegennimmt, ändert und weiterleitet.<sup>684</sup> Dadurch kann der Nutzer gegenüber einem anderen *Webserver* mit einer anderen als seiner eigenen *IP-Adresse* in Erscheinung treten.<sup>685</sup> Wird beim Abruf einer Webseite ein *Proxy-Server* ausgewählt, dessen Standort sich innerhalb des jeweiligen Empfangsgebietes befindet, kann die Geo-Sperre den Zugang zu den geschützten Inhalten i.d.R. nicht verhindern.<sup>686</sup>

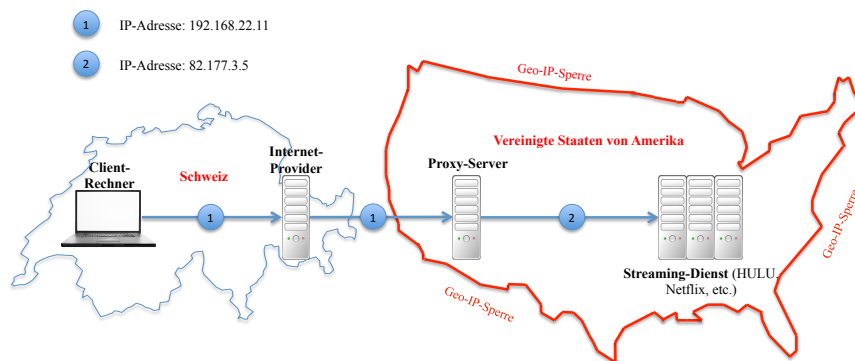


Abbildung 9: Umgehung einer Geo-IP-Sperre durch Zwischenschaltung eines Proxy Servers, Quelle: <<https://privacyknowledge.org/blog/wie-funktioniert-ein-proxy-server-zur-anonymisierung>> (besucht 3.7.2015)

### c) *Virtual Private Network (VPN)*

Die VPN-Dienste stellen den Nutzern *Serverkapazitäten* zur Verfügung, 276 deren Standorte sich irgendwo auf der Welt befinden und über die der ge-

<sup>684</sup> HILGERT/GRETH, 115; PRILL, 45; REINBACHER, HFR 2012, 184, spricht deshalb davon, dass der *Proxy-Server* lediglich als Mittler fungiert; MITSCHÖRFFER/GUTFLEISCH, MMR 2009, 732.

<sup>685</sup> WULLSCHLEGER, Rz. 251; HILGERT/GRETH, 115, REINBACHER, HFR 2012, 184; MITSCHÖRFFER/GUTFLEISCH, MMR 2009, 732.

<sup>686</sup> REINBACHER, HFR 2012, 184; MITSCHÖRFFER/GUTFLEISCH, MMR 2009, 732; durch die Installation bestimmter *Browser-Add-ons* wie etwa *FoxyProxy* oder *Stealthy* können Geo-Sperren mit noch geringerem Aufwand umgangen werden, als dies etwa bei manuellen Proxy-Konfigurationen der Fall ist.

### 3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers

samte Internetverkehr des Nutzers abgewickelt wird.<sup>687</sup> Beim Abruf eines *Webservers* erhält dieser nicht die tatsächliche IP-Adresse des Nutzers, sondern diejenige eines ausgewählten *Servers*.<sup>688</sup> Dadurch können Geo-Sperren zuverlässig umgangen werden.<sup>689</sup>

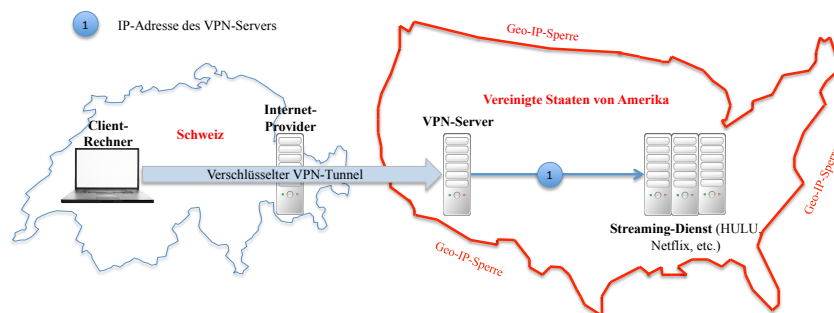


Abbildung 10: Umgehung einer Geo-IP-Sperre durch Zwischenschaltung eines Proxy Servers, Quelle: <<https://privacyknowledge.org/blog/wie-funktioniert-ein-proxy-server-zur-anonymisierung>> (besucht 3.7.2015)

## C. Rechtliche Bewertung der Umgehung von Geo-Sperren

### a) Strafbarkeit der Umgehung von Geo-Sperren nach URG

- 277 Die Beantwortung der Frage, ob die Umgehung einer Geo-Sperre urheberstrafrechtliche Konsequenzen nach sich zieht, hängt entscheidend davon ab, ob diese Sperren als wirksame technische Massnahmen i.S.v. Art. 39a Abs. 2 URG zu qualifizieren sind bzw. ob überhaupt eine Umgehungshandlung

<sup>687</sup> HILGERT/GRETH, 115, dabei werden räumlich getrennte Rechner über das Internet so zusammengeschaltet, dass sie wie in einem lokalen Netzwerk kommunizieren; SCHEDER-BIESCHIN, 74; REINBACHER, HFR 2012, 184; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 732.

<sup>688</sup> WULLSCHLEGER, Rz. 250; HILGERT/GRETH, 115, „der Datenabruf erfolgt dann über die innerhalb des virtuellen privaten Netzwerks zugeteilte *IP-Adresse*“; KUROSE/ROSS, 754 f.; PRILL, 46 f.; SCHEDER-BIESCHIN, 74; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 732; <[http://www.cyberghostvpn.com/de\\_de/vorteile](http://www.cyberghostvpn.com/de_de/vorteile)> oder <<https://www.blackvpn.com>> (beide besucht 25. August 2015).

<sup>689</sup> SCHEDER-BIESCHIN, 74; REINBACHER, HFR 2012, 184; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 732.



i.S.v. Art. 39a Abs. 1 URG vorliegt, wenn Geo-Sperren unter Verwendung von Anonymisierungsdiensten umgangen werden.

aa) *Geo-Sperren als wirksame technische Massnahmen i.S.v. Art. 39a Abs. 2 URG?*

Gemäss Art. 39a Abs. 1 URG dürfen wirksame technische Massnahmen zum Schutz von Werken und anderen Schutzobjekten nicht umgangen werden. 278 Geschützt sind gem. Art. 39a Abs. 2 URG nur wirksame technische Massnahmen. Die Anforderungen an die Wirksamkeit sollen nach h.L. nicht zu hoch angesetzt werden.<sup>690</sup> Demnach soll eine wirksame technische Massnahme bereits dann vorliegen, wenn diese geeignet ist, den durchschnittlichen Benutzer davon abzuhalten, eine Handlung vorzunehmen, die bestimmungsgemäss verhindert werden soll.<sup>691</sup> Das blosse Vorhandensein von Angeboten zur Umgehung technischer Massnahmen und deren leichte Erreichbarkeit über das Internet sollen deshalb noch nicht genügen, um die Wirksamkeit einer technischen Massnahme zu verneinen.

Geo-Sperren dienen dem Zweck, den Zugriff auf bestimmte Werke ausserhalb eines bestimmten Gebietes zu unterbinden und sind grundsätzlich geeignet, den Werkzugang auf ein bestimmtes Territorium zu begrenzen (Zugangsschranken).<sup>692</sup> Als Argument für die Annahme einer wirksamen technischen Massnahme bei Geo-Sperren wird vorgebracht, dass deren Umgehung nur einem kleinen Kreis von versierten Internetnutzern zugänglich sei.<sup>693</sup> Diese Ansicht abzulehnen, da bei Geo-Sperren schon deshalb nicht von wirksamen technischen Massnahmen gesprochen werden kann, weil diese ohne besondere technische Kenntnisse und unter geringem zeitlichen Aufwand – etwa durch Installation einer Anonymisierungssoftware oder Verwendung eines *Proxy-Servers* – umgangen werden können.<sup>694</sup> Dabei gilt 279

---

<sup>690</sup> AUF DER MAUR, SHK URG, Art. 39a N 2; REHBINDER/VIGANÒ, Art. 39a N 13; BARRELET/EGLOFF, Art. 39a N 8.

<sup>691</sup> AUF DER MAUR, SHK URG, Art. 39a N 2; REHBINDER/VIGANÒ, Art. 39a N 13; BARRELET/EGLOFF, Art. 39a N 8; HILTY, Urheberrecht, Rz. 432.

<sup>692</sup> PRILL, 51 f.; REINBACHER, HFR 2012, 186; MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 734 f.

<sup>693</sup> PRILL, 114 ff.

<sup>694</sup> HILGERT/GRETH, 116, wonach mittels Geo-Sperren „keine technische geographische Eingrenzung des Audio- oder Videostreams erreicht [wird]“, vielmehr werde lediglich „der Zugang aus bestimmten geographischen Regionen erschwert“, JANISCH/LACHENMANN, MMR-Aktuell 2013, 352345; REINBACHER, HFR 2012, 186; HOEREN, MMR 2007, 6; a.A. VON ALBRECHT/MUTSCHLER-SIEBERT/BOSCH, ZUM 2012, 97.

es zu berücksichtigen, dass weder Anonymisierungsdienste noch *Proxy-Server* oder *VPN-Clients* als Umgehungswerkzeuge i.S.v. Art. 39a Abs. 3 URG zu qualifizieren sind, weil deren Hauptzweck gerade nicht die Umgehung technischer Massnahmen, sondern der Schutz der Privatsphäre des Nutzers ist.<sup>695</sup>

- 280 MITSCHDÖRFFER/GUTFLEISCH bezweifeln zwar nicht die Wirksamkeit von Geo-Sperren, verneinen aber das Vorliegen einer Umgehungshandlung, weil die Geo-Sperren bloss den mutmasslichen Standort anhand der IP-Adresse desjenigen Rechners bestimmen, von dem die Anfrage unmittelbar stammt und basierend darauf entscheiden, ob die abgerufenen Inhalte übermittelt werden. Verwendet ein Nutzer zur Verschleierung seiner Identität bzw. seines Aufenthaltsortes einen *Proxy-Server* oder einen *VPN-Client*, werden jeweils die IP-Adressen des zwischengeschalteten *Proxy-Servers* oder *VPN-Clients* korrekt übertragen und geprüft. Die Geo-Sperre wird dabei „weder ausgeschaltet noch manipuliert“.<sup>696</sup>
- 281 Erfolgt der Zugriff auf eine Datei nicht über einen *Web-Server*, sondern direkt mittels *Deep-Link*, wird die Geo-Sperre i.d.R. ohnehin nicht umgangen, da eine Kontrolle der IP-Adresse nur dann erfolgt, wenn die Anfrage über einen *Web-Server* aufgebaut wird.<sup>697</sup>

*bb) Scheitern einer Strafbarkeit nach Art. 69a Abs. 1 lit. a URG*

- 282 Selbst wenn Geo-Sperren als wirksame technische Massnahme qualifiziert würden, scheitert eine Strafbarkeit nach Art. 69a Abs. 1 lit. a URG regelmässig an dem in letztgenannter Bestimmung statuierten Absichtserfordernis.<sup>698</sup> Die Umgehung wirksamer technischer Massnahmen ist nur dann strafbar, wenn diese mit der Absicht vorgenommen wird, „eine gesetzlich unerlaubte Verwendung von Werken und anderen Schutzobjekten vorzunehmen“. Soweit die Umgehung der Geo-Sperre lediglich zum Zwecke einer privaten Werkverwendung im Rahmen von Art. 19 Abs. 1 lit. a URG vorgenommen wird, ist eine Bestrafung nach Art. 69a Abs. 1 lit. a URG ausgeschlossen.

---

<sup>695</sup> Der *Download* einer entsprechenden Anonymisierungssoftware ist daher auch nicht nach Art. 69a Abs. 1 lit. b URG strafbar.

<sup>696</sup> Zum Ganzen MITSCHDÖRFFER/GUTFLEISCH, MMR 2009, 735.

<sup>697</sup> PRILL, 116, welche diesbezüglich auf eine Ähnlichkeit zur sog. „analogen Lücke“ verweist.

<sup>698</sup> S.o. Rz. 242.

*cc) Strafantragsberechtigung*

Nicht unproblematisch wäre in der vorliegenden Konstellation überdies auch die Frage nach der Berechtigung zur Stellung eines Strafantrags nach Art. 69a Abs. 1 lit. a URG bei grenzüberschreitenden Sachverhalten. Will ein Streaming-Dienst durch Verwendung von Geo-Sperren die Empfangbarkeit seines Angebots auf ein bestimmtes Territorium beschränken, besitzt typischerweise die entsprechenden Rechte für die Distribution der Werke ausserhalb dieses Gebietes gerade nicht. Die Rechteinhaber sind in diesem Fall nicht identisch mit derjenigen Person, welche die Geo-Sperre einsetzt. Richtigerweise sollte für die Antragsberechtigung nur die Rechtsinhaberschaft an den betreffenden Urheberrechten und verwandten Schutzrechten in der Schweiz entscheidend sein, nicht jedoch der Umstand, dass jemand technische Schutzmassnahmen anwendet.<sup>699</sup>

***b) Strafbarkeit der Umgehung von Geo-Sperren nach StGB***

*aa) Unbefugte Datenbeschaffung (Art. 143 StGB)*

Für eine unbefugte Datenbeschaffung nach Art. 143 StGB wird vorausgesetzt, dass der Datenberechtigte die zumutbaren und in der konkreten Situation üblichen Massnahmen getroffen hat, damit die Daten vor einem unerlaubten Zugriff besonders gesichert sind.<sup>700</sup> Das Vorliegen einer besonderen Zugriffssicherung ist bei Geo-Sperren abzulehnen: Anders als passwortgesicherte Zugangsschranken lässt sich diese mit geringem zeitlichen und technischen Aufwand umgehen.<sup>701</sup> Folglich erfüllt die Umgehung einer Geo-Sperre mittels Anonymisierungsdiensten, *Proxy-Servern* oder *VPN-Clients* den objektiven Tatbestand von Art. 143 StGB nicht.

*bb) Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143<sup>bis</sup> StGB)*

Ebenso wie Art. 143 StGB setzt auch der Tatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem voraus, dass das System gegen

---

<sup>699</sup> Vgl. BARRELET/EGLOFF, Art. 69a N 3; GLARNER, sic! 2006, 650; zum deutschen Recht PRILL, 117 f.; a.A. MITSCHKE/GRUTTMANN, MMR 2009, 735.

<sup>700</sup> WEISSENBERGER, BSK StGB II, Art. 143 N 18 f.; DONATSCH, Strafrecht III, 196; TRECHSEL/CRAMER, PK StGB, Art. 143 N 6; STRATENWERTH/JENNY/BOMMER, § 14 N 29.

<sup>701</sup> HILGERT/GRUTH, 115 f.; REINBACHER, HFR 2012, 188; HOEREN, MMR 2007, 6.

den unbefugten Zugriff Dritter besonders gesichert ist.<sup>702</sup> Wie bereits zuvor ausgeführt wurde, ist bei Geo-Sperren das Vorliegen einer besonderen Zugriffssicherung abzulehnen, weshalb vorliegend keine Bestrafung nach Art. 143<sup>bis</sup> StGB möglich ist.

cc) *Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)*

- 286 Die Umgehung einer Geo-Sperre erfüllt den Tatbestand des betrügerischen Missbrauchs einer Datenverarbeitungsanlage i.S.v. Art. 147 StGB, sofern die Verschleierung der *IP-Adresse* mittels *Proxy-Servern* oder *VPN-Clients* als unrichtige Verwendung von Daten zu qualifizieren ist. Dagegen lässt sich allerdings einwenden, dass die *IP-Adressen* des verwendeten *Proxy-Servers* bzw. *VPN-Clients* korrekt übermittelt werden. Es steht den Anbietern von Geo-Sperren insbesondere frei, zumindest den Zugang für *IP-Adressen* von frei verfügbaren *Proxy-Servern* zu sperren.<sup>703</sup>

dd) *Erschleichen einer Leistung (Art. 150 StGB)*

- 287 Bei kostenlosen Angeboten fällt eine Strafbarkeit nach Art. 150 StGB bereits deshalb ausser Betracht, weil das Tatbestandserfordernis der Entgeltlichkeit der Leistung nicht erfüllt ist. Bei kostenpflichtigen Angeboten werden von den Stream-Anbietern kumulativ Zugangsschranken eingesetzt. Solange der Nutzer die geforderte Gebühr für die Nutzung der geschützten Inhalte entrichtet, ist zumindest fraglich, ob überhaupt eine Leistungserschleichung vorliegt.

ee) *Herstellen und Inverkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote (Art. 150<sup>bis</sup> StGB)*

- 288 Die zur Verschleierung der *IP-Adresse* erforderlichen Programme sind nicht als Umgehungswerkzeuge i.S.v. Art. 150<sup>bis</sup> StGB zu qualifizieren, da diese nicht zur unbefugten Entschlüsselung codierter Rundfunkprogramme oder Fernmeldedienste bestimmt und geeignet sind.<sup>704</sup> Eine Strafbarkeit nach Art. 150<sup>bis</sup> StGB ist deshalb ausgeschlossen.

---

<sup>702</sup> WEISSENBERGER, BSK StGB II, Art. 143<sup>bis</sup> N 14 ff.; STRATENWERTH/WOHLERS, Art. 143<sup>bis</sup> N 1; TRECHSEL/CRAMERI, PK StGB, Art. 143<sup>bis</sup> N 5 StGB.

<sup>703</sup> REINBACHER, HFR 2012, 188.

<sup>704</sup> FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 26 f.; STRATENWERTH/JENNY/BOMMER, § 16 N 59.

**c) *Fazit zur Umgehung von Geo-Sperren***

Die Umgehung von Geo-Sperren zum Zwecke des Zugriffs auf urheberrechtlich geschützte Inhalte zieht weder eine Sanktionierung nach den Strafbestimmungen des URG noch eine Bestrafung nach den einschlägigen Normen des StGB nach sich. 289

**8. Herunterladen von Audio-/Video-Streams mittels Streamripper, Recorder-Software und Konvertierungsdiensten**

Es existieren verschiedene Softwareprogramme, die es den Nutzern ermöglichen, gestreamte Inhalte von legalen Streaming-Portalen wie YouTube, Clipfish, MyVideo etc. sowie von Webradio-Programmen herunterzuladen, um diese zu einem späteren Zeitpunkt (offline) wiederzugeben.<sup>705</sup> Konvertierungsdienste ermöglichen etwa, dass die Tonspur aus Videoclips herausgefiltert und in ein gewünschtes Dateiformat (z.B. in eine MP3-Datei) umgewandelt und abgespeichert werden kann.<sup>706</sup> 290

**A. Technische Einführung**

Eine gängige Methode ist das *URL-Verfahren*, bei dem der Nutzer die Internetadresse der gewünschten digitalen Werkdatei in ein dafür vorgesehenes Feld kopiert und danach mit wenigen Mausklicks das Konvertieren der Audio-/Video-Datei veranlassen und diese anschliessend als „reine“ Audio-Datei auf ein beliebiges Speichermedium herunterladen kann.<sup>707</sup> Bei gewissen Konvertierungsdiensten ist zudem eine Suchfunktion vorhanden, die es den Nutzern ermöglicht, durch Eingabe bestimmter Suchbegriffe (z.B. Interpret, Song- bzw. Videotitel), ausgewählte Streaming-Dienste im Internet (z.B. *YouTube*, *Dailymotion*, *Vevo*, *Clipfish* usw.) zu durchsuchen, um die Inhalte anschliessend in das gewünschte Zielformat zu konvertieren.<sup>708</sup> Bestimmte Softwareprogramme durchsuchen vollautomatisch tausende von Internetradios nach 291

---

<sup>705</sup> HILGERT/GRETH, 119 f.; PRILL, 32; JANISCH/LACHENMANN, MMR 2013, 213; REDLICH, K&R 2012, 713; KOCH, GRUR 2010, 578; VON ZIMMERMANN, MMR 2007, 553.

<sup>706</sup> HILGERT/GRETH, 119 f.; PRILL, 32 f.; JANISCH/LACHENMANN, MMR 2013, 213 f.

<sup>707</sup> Wie etwa <<http://convert2mp3.net>>, <<https://www.onlinevideoconverter.com/de/video-converter>> oder <<http://www.video2mp3.de/de/>> (alle besucht 25. August 2015).

<sup>708</sup> JANISCH/LACHENMANN, MMR 2013, 214; <<http://convert2mp3.net>> (besucht 25. August 2015).

ausgewählten Musikstücken, die sodann heruntergeladen werden.<sup>709</sup> Mit der Software *Audials Moviebox* können mittels Streaming-Technologie übertragene Audio-/Video-Dateien aufgezeichnet und abgespeichert werden.<sup>710</sup> Sämtliche der oben erwähnten Programme verfolgen im Kern den Zweck der Herstellung dauerhafter Werkkopien.

- 292 Bei Softwareprogrammen, welche direkt auf dem Nutzerrechner installiert werden, wird die Werkkopie unmittelbar auf einem Speichermedium beim Nutzer abgespeichert.<sup>711</sup> Bei *serverbasierten* Konvertierungsdiensten wird die gestreamte Datei zunächst im gewünschten Format auf dem *Server* des Diensteanbieters zwischengespeichert und kann anschliessend (meist innerhalb einer gewissen Zeitspanne) vom Nutzer über einen individuellen *Download-Link* heruntergeladen werden.<sup>712</sup>

## **B. Rechtliche Bewertung des Einsatzes von Konvertierungsdiensten und Aufnahmesoftware nach URG**

- 293 Nachfolgend wird die Urheberrechtskonformität der Konvertierung von Streaming-Angeboten untersucht sowie die Rechtmässigkeit der Herstellung dauerhafter Werkkopien mittels sog. Stream-Recorder aufgezeigt. In einem zweiten Schritt wird untersucht, inwieweit sich die Nutzer strafbar machen, wenn bei der Herstellung von Werkkopien wirksame technische Massnahmen (Kopiersperren) umgangen werden.<sup>713</sup> Schliesslich soll die Zulässigkeit des Anbietens und der Beschaffung entsprechender Umgehungswerkzeuge zur Herstellung dauerhafter Werkvervielfältigungen von gestreamten Werken aus rechtlicher Perspektive beleuchtet werden.

---

<sup>709</sup> <<http://audials.com/de/radiotracker/index.html>> (besucht 25. August 2015); ausführlich dazu PRILL, 32 ff.

<sup>710</sup> <<http://audials.com/de/moviebox/index.html#streaming>> (besucht 25. August 2015).

<sup>711</sup> PRILL, 32 f.; JANISCH/LACHENMANN, MMR 2013.

<sup>712</sup> REDLICH, K&R 2012, 715; Die Unterscheidung zwischen Programmen, die zuerst heruntergeladen und installiert werden müssen und *serverbasierten* Konvertierungsdiensten gilt es mit Blick auf das weitgehende Verbot von Vorbereitungshandlungen nach Art. 39a Abs. 3 URG zu beachten.

<sup>713</sup> Z.B. *RTMPE* (Encrypted Real Time Messaging Protocol) von Adobe; *EME* (Encrypted Media Extensions) des World Wide Web Consortium (W3C) zur Streaming-Verschlüsselung für *HTML5*; <<https://w3c.github.io/encrypted-media>> (besucht 25. August 2015); HILGERT/GRETH, 104.

**a) *Unerlaubte Werkänderung***

Gemäss Art. 11 Abs. 1 lit. a URG hat der Urheber das ausschliessliche Recht zu bestimmen, ob, wann und wie das Werk geändert werden darf. Eine unerlaubte Werkänderung wird nach Art. 67 Abs. 1 lit. c URG mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft. Wird ein gestreamter Film mit einer Aufnahmesoftware, einem sog. Streaming-Recorder aufgezeichnet, ist es zumindest fraglich, ob dieser Vorgang überhaupt als Werkänderung zu qualifizieren ist, sofern keine Änderungen in qualitativer Hinsicht vorgenommen werden.<sup>714</sup>

Die Konvertierung in ein anderes Dateiformat (z.B. von einer MP4-Datei in eine MP3-Datei) stellt demgegenüber nicht bloss eine technische Umwandlung eines Werks dar, sondern ist m.E. als urheberrechtlich relevante Werkänderung i.S.v. Art. 11 Abs. 1 lit. a URG zu qualifizieren.<sup>715</sup> Gestützt auf die Schrankenregelung von Art. 19 Abs. 1 lit. a URG ist jede Werkverwendung im persönlichen Gebrauch und im Kreis von Personen, die unter sich eng verbunden sind, erlaubt. Darunter fällt auch das Recht, Änderungen am Werk vorzunehmen.<sup>716</sup> Vorausgesetzt, dass sämtliche Werkänderungen, die bei der Konvertierung bzw. der Aufnahme der gestreamten Werke vorgenommen werden, innerhalb des Privatgebrauchs stattfinden, sind diese durch die Schrankenregelung zum Privatgebrauch nach Art. 19 Abs. 1 lit. a URG gedeckt.

**b) *Unerlaubte Herstellung von Werkexemplaren***

Die durch Verwendung von Konvertierungsdiensten oder Aufnahmesoftware hergestellten dauerhaften Werkvervielfältigungen tangieren das in Art. 10 Abs. 2 lit. a URG statuierte, ausschliessliche Vervielfältigungsrecht des Urhebers. Sofern keine Einwilligung der Rechteinhaber für die Herstellung des Werkexemplars vorliegt bzw. sich der Nutzer bei der Herstellung der Werkkopie nicht auf eine Schrankenregelung des Urheberrechts berufen kann,

---

<sup>714</sup> PFORTMÜLLER, SHK URG, Art. 11 N 4; BARRELET/EGLOFF, Art. 11 N 6a, wonach die Umcodierung oder Digitalisierung einer analogen Audio-/Video-Aufzeichnung nicht als Änderung i.S.v. Art. 11 URG zu qualifizieren sei.

<sup>715</sup> Vgl. dazu die Ausführungen bei PFORTMÜLLER, SHK URG, Art. 11 N 3.

<sup>716</sup> Botschaft URG 1989, 539; CHERPILLOD, SIWR II/1, 264 f.; DAVID, SHK URG, Art. 19 N 9; BARRELET/EGLOFF, Art. 9 N 7 und Art. 19 N 11, „Vorbehalten bleibt einzig der harte Kern des Urheberpersönlichkeitsrechts“; REHBINDER/VIGANÒ, Art. 19 N 20; GASSER, 66 ff.

liegt eine unerlaubte Herstellung von Werkexemplaren nach Art. 67 Abs. 1 lit. e URG vor. Da es sich um dauerhafte Vervielfältigungen handelt, ist die Schranke für ausschliesslich technisch bedingte Kopien ohne eigene wirtschaftliche Bedeutung nach Art. 24a URG nicht anwendbar. Die Vervielfältigung von urheberrechtlich geschützten Werken zum Privatgebrauch ist jedoch gestützt auf die in Art. 19 Abs. 1 lit. a URG verankerte Schrankenregelung zugunsten des Privatgebrauchs zulässig. Dabei ist es irrelevant, ob die Kopiervorlage rechtmässig zugänglich gemacht wurde.<sup>717</sup>

**c) *Verbot der Umgehung technischer Massnahmen***

297 Auch wenn bei der Datenübertragung mittels Streaming im Normalfall nur vorübergehende Vervielfältigungen i.S.v. Art. 24a URG hergestellt werden, die nicht ohne Weiteres dauerhaft abgespeichert werden können, kann in der Anwendung der Streaming-Technik noch keine wirksame technische Massnahme zum Schutze eines Werks i.S.v. Art. 39a Abs. 2 URG gesehen werden.<sup>718</sup>

298 Für das Vorliegen einer wirksamen technischen Massnahme müssen zusätzlich wirksame Verschlüsselungstechniken zum Einsatz gelangen.<sup>719</sup> Die Wirksamkeit einer Verschlüsselungstechnik ist nicht bereits dann widerlegt, wenn diese zum ersten Mal umgangen wird – ansonsten würde die Strafbestimmung von Art. 69a Abs. 1 lit. a URG praktisch leerlaufen.<sup>720</sup> REDLICH schliesst aber aus der Vielzahl der verfügbaren Angebote zur Herstellung dauerhafter Werkkopien von gestreamten Werken, dass die Stream-Anbieter regelmässig keine wirksamen technischen Massnahmen einsetzen würden.<sup>721</sup>

---

<sup>717</sup> S.o. Rz. 203 ff.; GASSER, SHK URG, Art. 19 N 10b; BARRELET/EGLOFF, Art. 19 N 7b; BAUMGARTNER, 200.

<sup>718</sup> REDLICH, K&R 2012, 716, vergleicht die Situation der Aufnahme eines ungeschützten Streams mit der Herstellung dauerhafter Aufzeichnungen von TV-/Radiosendungen mittels Kassetten-, Video- oder DVD-Recordern, welche ebenfalls nicht als Umgehung einer wirksamen technischen Massnahme zu qualifizieren sind, solange dabei keine Nutzungs- oder Zugangsschranken umgangen werden.

<sup>719</sup> Ebenso JANISCH/LACHENMANN, MMR 2013, 214; REDLICH, K&R 2012, 716 f.

<sup>720</sup> REHBINDER/VIGANÒ, Art. 39a N 13; zum deutschen Recht REDLICH, K&R 2012, 716.

<sup>721</sup> REDLICH, K&R 2012, 716 f., der Autor schlägt vor, ggf. das Vorliegen der Wirksamkeit einer technischen Massnahme unter Hinzuziehung sachverständiger Begutachtung im Einzelfall zu prüfen. An diesem Lösungsansatz ist zu kritisieren, dass er aus Sicht der Konsumenten zu Rechtsunsicherheiten führt, weil der Nutzer im Zeitpunkt der Vornahme der Umgehungshandlung noch gar nicht Bescheid weiss über die Wirksamkeit der technischen Massnahme.



Auch HEINEMEYER/KREITLOW weisen darauf hin, dass die derzeit eingesetzten Verschlüsselungstechniken zumindest teilweise nicht mehr dem aktuellsten Stand der Technik entsprechen würden und zudem aus kryptografischer Sicht eklatante Mängel aufweisen würden.<sup>722</sup> Gemäss Art. 39a Abs. 4 URG kann das Umgehungsverbot nicht gegenüber denjenigen Personen geltend gemacht werden, welche die Umgehung ausschliesslich zum Zweck einer gesetzlich erlaubten Verwendung vornehmen.<sup>723</sup> Darunter fällt nach Art. 19 Abs. 1 lit. a URG jede Werkverwendung im persönlichen Bereich und im Kreis von Personen, die unter sich eng verbunden sind – mitunter also auch die Herstellung von Privatkopien. Im Ergebnis ist daher festzuhalten, dass aufgrund der tatbestandsausschliessenden Wirkung von Art. 39a Abs. 4 URG das Verbot der Umgehung technischer Massnahmen gegenüber Personen, welche technische Massnahmen ausschliesslich zum Zweck einer gesetzlich erlaubten Verwendung umgehen, nicht geltend gemacht werden kann.<sup>724</sup>

#### **d) Verbot von Vorbereitungshandlungen**

Während der Besitz zum Eigengebrauch von Vorrichtungen zur Umgehung technischer Massnahmen straflos bleibt, statuiert der Gesetzgeber in Art. 39a Abs. 3 URG ein Verbot für das Herstellen, Einführen, Anbieten, Veräussern oder das sonstige Verbreiten, Vermieten, Überlassen zum Gebrauch sowie das Bewerben und den Besitz zu Erwerbszwecken von Umgehungswerkzeugen.<sup>725</sup> Durch dieses weitreichende Verbot wird es dem Privatanutzer faktisch weitgehend verunmöglicht, auf legale Weise eine wirksame technische Massnahme zu umgehen, weil er die dazu erforderlichen Werkzeuge nicht auf legale Weise beschaffen kann.

Wird das Umgehungswerkzeug von einem *Server* im Inland heruntergeladen, liegt keine urheberstrafrechtlich relevante Handlung vor, doch hat sich in dieser Konstellation der Anbieter nach Art. 69a Abs. 1 lit. b URG strafbar gemacht.<sup>726</sup> Die Frage, ob das Herunterladen eines Umgehungswerkzeugs von einem ausländischen *Server* als *Einführen* i.S.v. Art. 39a Abs. 3 lit. c

---

<sup>722</sup> So etwa die *RTMPE*-Verschlüsselung des Herstellers Adobe; vgl. HEINEMEYER/KREITLOW, MMR 2013, 625 f.

<sup>723</sup> SCHWARZENEGGER, ZSR 2008 II, 500 f.; BARRELET/EGLOFF, Art. 69a N 5.

<sup>724</sup> AUF DER MAUR, SHK URG, Art. 39a N 14; DAVID, SHK URG, Art. 69a N 8; Botschaft URG 2006, 3425.

<sup>725</sup> AUF DER MAUR, SHK URG, Art. 39a N 12; REHBINDER/VIGANÒ, Art. 39a N 22; BARRELET/EGLOFF, Art. 39a N 9.

<sup>726</sup> AUF DER MAUR, SHK URG, Art. 39a N 12.

3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers

---

URG zu qualifizieren ist, wird in der Lehre und Rechtsprechung uneinheitlich beantwortet. PLATZ ist der Ansicht, dass beim blossen *Download* nicht von einer Einfuhr im herkömmlichen Sinne gesprochen werden könne, da diese eine physische Verschiebung von Datenträgern voraussetzen würde.<sup>727</sup> Anderer Meinung ist AUF DER MAUR, der dafür plädiert, dass auch das Herunterladen eines solchen Umgehungswerkzeugs von einem ausländischen *Server* eine verbotene Importhandlung darstellen würde.<sup>728</sup>

- 301 Die Umgehung einer technischen Massnahme zum Zweck einer gesetzlich erlaubten Verwendung bleibt aufgrund des Vorbehalts erlaubter Verwendungen von Art. 39a Abs. 4 URG straffrei. Indessen macht sich der Nutzer u.U. strafbar, wenn er sich zur Umgehung einer technischen Massnahme ein entsprechendes Werkzeug (Computerprogramm) von einem ausländischen *Server* auf seinen Rechner herunterlädt. Schliesslich gilt es zu beachten, dass Art. 69a Abs. 1 lit. b URG nur die vorsätzliche Beschaffung von Umgehungswerkzeugen unter Strafe stellt. Mit Blick auf das *protected streaming*, bei dem die gestreamten Inhalte verschlüsselt übertragen werden, ist zumindest fraglich, ob sich der Durchschnittsnutzer überhaupt bewusst ist, dass bei der Aufzeichnung des Streams eine wirksame technische Schutzmassnahme umgangen wird. Sodann ist unklar, wer zur Stellung des Strafantrags berechtigt sein soll. Da die Beschaffung des Umgehungswerkzeuges typischerweise im Vorfeld der eigentlichen Umgehungshandlung stattfindet, existieren noch keine „in ihrem Schutz“ verletzte Personen nach Art. 69a Abs. 1 lit. b URG.<sup>729</sup>
- 302 Zahlreiche Konvertierungsdienste können direkt online genutzt werden.<sup>730</sup> Da bei der Verwendung webbasierter Konvertierungsdienste kein Softwareprogramm heruntergeladen werden muss, liegt auch kein Einführen eines Umgehungswerkzeugs i.S.v. Art. 39a Abs. 3 i.V.m. Art. 69a Abs. 1 lit. b URG vor, womit eine strafbare Vorbereitungshandlung ausser Betracht fällt.

---

<sup>727</sup> PLATZ, Jusletter vom 16. Juni 2008, Rz. 4.

<sup>728</sup> AUF DER MAUR, SHK URG, Art. 39a N 12; ebenso RUBLI, Rz. 366, der sowohl den Postversand als auch die elektronische Übermittlung von der Tathandlung der Einfuhr mitumfasst sieht.

<sup>729</sup> Vgl. SCHWARZENEGGER, ZSR 2008 II, 491, mit dem Hinweis, dass die Antragsberechtigung weit gefasst werden muss und entsprechend jedem potentiell betroffenen Urheber eine Antragsberechtigung zugesprochen werden müsste, damit die Norm nicht bloss toter Buchstabe bleibt.

<sup>730</sup> <<http://convert2mp3.net>>, <[www.clipconverter.cc/de](http://www.clipconverter.cc/de)> (beide besucht 25. August 2015); siehe HILGERT/GRETH, 119 ff., m.w.H.

e) *Analoge Lücke*

Durch technische Schutzmassnahmen können nur digitale, nicht aber analoge Vervielfältigungen verhindert werden.<sup>731</sup> Der Begriff analoge Lücke bezeichnet die Tatsache, dass technische Massnahmen keinen wirksamen Schutz gegen die Herstellung analoger Vervielfältigungen bieten.<sup>732</sup> Folglich liegt bei der Herstellung einer analogen Kopie eines durch technische Massnahmen geschützten Werks keine Umgehung einer wirksamen technischen Massnahme vor.<sup>733</sup> Dabei ist es unerheblich, ob das analoge Signal innerhalb des Rechners (auf der sog. Netzwerkschicht oder über das Windows Grafiksystem) oder durch externe Geräte (Kamera, Mikrofon etc.) abgegriffen wird, da die technischen Schutzmassnahmen in beiden Fällen nicht wirksam sind.<sup>734</sup>

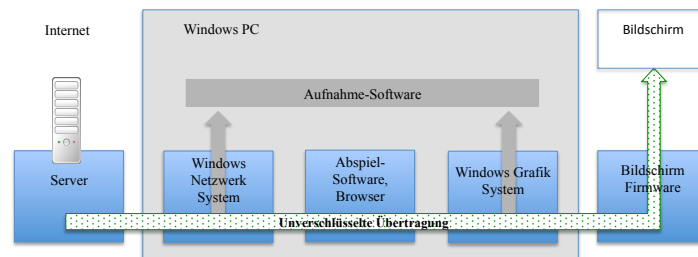


Abbildung 11: Aufnahme eines Videostreams mit ungeschützter Übertragung und ungeschütztem Abspielen  
Quelle: <[http://audials.com/de/audials/unternehmen-audials-ag/rechtliche\\_hinweise.html](http://audials.com/de/audials/unternehmen-audials-ag/rechtliche_hinweise.html)> (besucht 3.7.2015)

Gewisse Programme ermöglichen auch die Aufzeichnung von verschlüsselten Streams (z.B. durch das neue Streaming-Verfahren EME), ohne dass dabei technische Massnahmen umgangen werden. Konkret machen sich diese Programme den Umstand zunutze, dass die gestreamten Daten zwar zunächst verschlüsselt an den *Browser* übertragen werden, aber anschliessend im *Browser* des Nutzers entschlüsselt und ohne Kopierschutz an die Grafikkarte weitergeleitet werden. Da die Aufnahmesoftware einzig die un-

<sup>731</sup> WANDTKE/OHST, N 51 zu § 95a UrhG; JANISCH/LACHENMANN, MMR 2013, 215.

<sup>732</sup> DREIER/SCHULZE, N 15 zu § 95a UrhG; JANISCH/LACHENMANN, MMR 2013, 215; SPINDLER, FS-Weber, 792; GIRSBERGER, 215.

<sup>733</sup> Art. 69a Abs. 1 URG setzt die Umgehung einer technischen Massnahme voraus; vgl. zum deutschen Recht WANDTKE/OHST, N 51 zu § 95a UrhG; DREIER/SCHULZE, N 15 zu § 95a UrhG.

<sup>734</sup> WANDTKE/OHST, N 51 zu § 95a UrhG; JANISCH/LACHENMANN, MMR 2013, 215 m.w.H.

3. Teil: Rechtliche Bewertung der einzelnen Vorgänge beim Streaming von urheberrechtlich geschützten Werken aus Sicht des Nutzers

verschlüsselten Signale aufzeichnet und zu einer Videodatei zusammenfügt, liegt keine Umgehung einer technischen Massnahme vor.<sup>735</sup>

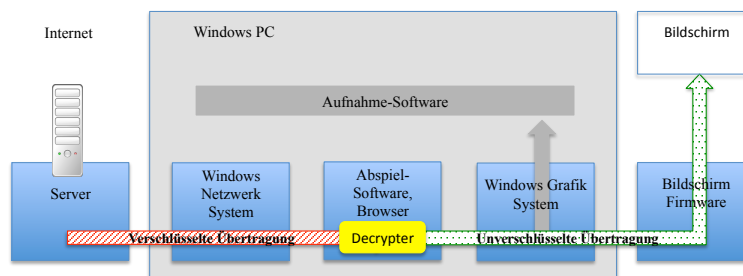


Abbildung 12: Aufnahme eines Videostreams mit geschützter Übertragung und ungeschütztem Abspielen  
Quelle: <[http://audials.com/de/audials/unternehmen-audials-ag/rechtliche\\_hinweise.html](http://audials.com/de/audials/unternehmen-audials-ag/rechtliche_hinweise.html)> (besucht 3.7.2015)

- 305 Beim sog. Anzeigeschutz werden die digitalen Inhalte dagegen nicht nur verschlüsselt an den *Browser* bzw. die Abspielsoftware übertragen, sondern darüber hinaus auch verschlüsselt an den Bildschirm weitergereicht. In diesen Fällen ist eine Aufnahme mittels Software nur unter Umgehung der technischen Massnahme möglich.<sup>736</sup>

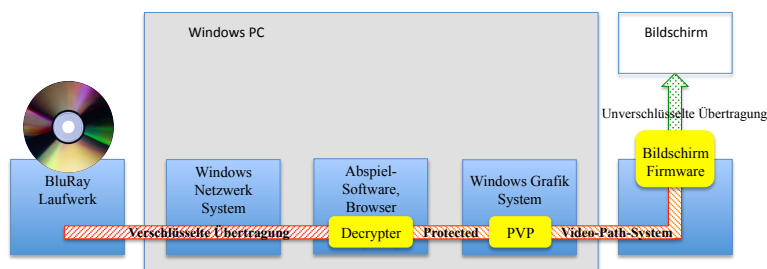


Abbildung 13: Aufnahme eines Videostreams mit geschützter Übertragung und geschütztem Abspielen  
(Hauptanwendungsfall BluRay-Disc)  
Quelle: <[http://audials.com/de/audials/unternehmen-audials-ag/rechtliche\\_hinweise.html](http://audials.com/de/audials/unternehmen-audials-ag/rechtliche_hinweise.html)> (besucht 3.7.2015)

- 306 Die Befürchtung, dass durch die Pönalisierung der Vorbereitungshandlungen zur Umgehung technischer Massnahmen die Nutzer faktisch um ihr Recht gebracht werden, Vervielfältigungen im Rahmen des Eigengebrauchs herzustellen, muss insoweit relativiert werden, als im Bereich der analogen Lücke immer straflos eine Privatkopie zum Eigengebrauch hergestellt werden

<sup>735</sup> WANDTKE/OHST, N 51 zu § 95a UrhG; STRÖMER/GASPER, K&R 2004, 17; PLEISTER/RUTTIG, MMR 2003, 765.

<sup>736</sup> <[http://audials.com/de/audials/unternehmen-audials-ag/rechtliche\\_hinweise.html](http://audials.com/de/audials/unternehmen-audials-ag/rechtliche_hinweise.html)> (besucht 3. Juli 2015).

kann.<sup>737</sup> Die Aufzeichnung analoger Signale mittels geeigneter Aufnahmegeräte zur Herstellung von Werkkopien kann durch technische Massnahmen nicht verhindert werden.<sup>738</sup>

### **C. Rechtliche Bewertung des Einsatzes von Konvertierungsdiensten und Aufnahmesoftware nach StGB**

#### **a) Unbefugte Datenbeschaffung (Art. 143 StGB)**

Auch bei der Annahme von echter Konkurrenz<sup>739</sup> zwischen Art. 69a URG <sup>307</sup> und Art. 143 StGB muss eine Strafbarkeit nach letztgenannter Bestimmung verneint werden, da es bereits an der Tatbestandsvoraussetzung der besonderen Sicherung gegen den unbefugten Zugang fehlt.<sup>740</sup> Weil der Nutzer bereits Zugang zum gestreamten Werk hat, liegt keine unbefugte Beschaffungshandlung vor. Sodann ist auch das Erfordernis der fehlenden Bestimmtheit für den Täter vorliegend nicht erfüllt, da die Audio-/Video-Dateien grundsätzlich für jedermann frei zugänglich sind.<sup>741</sup> Demzufolge ist das Vorliegen einer unbefugten Datenbeschaffung bei der Konvertierung bzw. Aufnahme eines urheberrechtlich geschützten digitalen Werkes unter Umgehung einer Nutzungsschranke (Kopierschutz) zu verneinen.

---

<sup>737</sup> Kritisch RUBLI, Rz. 471; GIRSBERGER, 207; BAUMGARTNER, 181 f.; BECHTOLD, Informationsrecht, 381 f.

<sup>738</sup> S.o. Rz. 217; etwaige – technisch bedingte – Qualitätseinbussen, die bei der Herstellung der Werkkopie bzw. einer anschliessenden Redigitalisierung entstehen, sind vom Nutzer hinzunehmen. Auch die Vervielfältigung analoger Werke, etwa bei der Herstellung von Fotokopien aus Büchern und Zeitschriften, ist mit Qualitätseinbussen verbunden.

<sup>739</sup> WEISSENBERGER, BSK StGB II, Art. 143 N 39; STRATENWERTH/JENNY/BOMMER, § 14 N 35; a.A. SCHWARZENEGGER, ZSR 2008 II, 499.

<sup>740</sup> Die Verschlüsselung des Streams dient lediglich als Kopierschutz (Nutzungsschranke) und nicht als Zugangsschranke; WEISSENBERGER, BSK StGB II, Art. 143 N 18 ff.; DONATSCH, Strafrecht III, 196; TRECHSEL/CRAMERI, PK StGB, Art. 143 N 6; STRATENWERTH/WOHLERS, Art. 143 N 2.

<sup>741</sup> Vgl. Art. 143 Abs. 1 StGB; Gewisse Einschränkungen können sich allenfalls bei Geosperren ergeben bzw. bei passwortgesicherten kostenpflichtigen Datenbanken. In der vorliegenden Konstellation wird jedoch nicht eine Zugangsschranke umgangen, sondern eine Nutzungsschranke (Kopierschutz) ausgehebelt; WEISSENBERGER, BSK StGB II, Art. 143 N 14 ff.; TRECHSEL/CRAMERI, PK StGB, Art. 143 N 5; STRATENWERTH/JENNY/BOMMER, § 14 N 28; Botschaft StGB 1991, 1010.

**b)      *Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)***

- 308 Bei sämtlichen Konvertierungsdiensten und Aufnahmeprogrammen, die sich bei der Herstellung dauerhafter Werkkopien die sog. analoge Lücke zunutze machen, ohne dabei durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen Datenverarbeitungs- oder Datenübermittlungsvorgang einzuwirken, fällt eine Strafbarkeit nach Art. 147 StGB ausser Betracht.
- 309 Der Einsatz einer entsprechenden Software zur Entschlüsselung eines kopiergeschützten Streams zum Zwecke der Herstellung dauerhafter Werkkopien könnte als *Einwirkung auf einen Datenübermittlungsvorgang mittels unbefugter, unvollständiger oder unbefugter Verwendung von Daten* qualifiziert werden.<sup>742</sup> Zur Erfüllung des Tatbestands von Art. 147 StGB muss einerseits unrechtmässig auf den Datenübermittlungsvorgang eingewirkt werden und sodann eine Vermögensverschiebung zum Schaden eines andern herbeigeführt bzw. eine Vermögensverschiebung „unmittelbar darnach“ verdeckt werden.<sup>743</sup> Da die Software zur Umgehung des Kopierschutzes keine Vermögensverschiebung bewirkt, sondern bloss die Aufzeichnung der verschlüsselt übertragenen Daten ermöglicht, ist das Vorliegen des betrügerischen Missbrauchs einer Datenverarbeitungsanlage i.S.v. Art. 147 StGB zu verneinen.

**c)      *Erschleichen einer Leistung (Art. 150 StGB)***

- 310 Die Bestimmung von Art. 150 StGB schützt das Vermögen des Anbieters einer Dienstleistung. In jenen Fällen, in denen die Stream-Anbieter die geschützten Werke kostenlos anbieten, fehlt es am Tatbestandserfordernis der Entgeltlichkeit des Angebots.<sup>744</sup> Bei kostenpflichtigen Streaming-Angeboten ist wiederum fraglich, ob überhaupt eine Leistungerschleichung vorliegt, wenn ein Nutzer die gesendeten Signale unter Verwendung entsprechender

---

<sup>742</sup> HEINEMEYER/KREITLOW, MMR 2013, 626 f., falls etwa die Daten zur Umgehung der Verschlüsselung mittels Reverse-Engineering ermittelt wurden und sich der Stream-Recorder gegenüber dem *Server* als autorisierter *Server* ausgibt, ohne dies tatsächlich zu sein.

<sup>743</sup> WEISSENBERGER, BSK StGB II, Art. 147 N 37 ff.; DONATSCH, Strafrecht III, 251 f.; TRECHSEL/CRAMERI, PK StGB, Art. 147 N 9 ff.; STRATENWERTH/WOHLERS, Art. 147 N 4.

<sup>744</sup> WEISSENBERGER, BSK StGB II, Art. 150 N 20; STRATENWERTH/WOHLERS, Art. 150 N 1; STRATENWERTH/JENNY/BOMMER, § 16 N 50.

Programme oder anderer Geräte aufzeichnet. Solange der Nutzer den Werkzugang legal erhalten hat, ist m.E. eine Leistungerschleichung nach Art. 150 StGB ausgeschlossen.

**D. Exkurs: Rechtliche Bewertung des Vertriebs von Umgehungswerkzeugen und der Erbringung von Dienstleistungen zur Umgehung technischer Massnahmen**

**a) Strafbarkeit nach URG**

Gemäss Art. 69a Abs. 1 lit. b URG sind der Vertrieb und das Bewerben von Umgehungswerkzeugen sowie die Erbringung von Dienstleistungen zur Umgehung wirksamer technischer Schutzmassnahmen verboten.<sup>745</sup> Dass die Umgehungswerkzeuge tatsächlich eingesetzt werden, ist für die Erfüllung des Tatbestandes nicht erforderlich.<sup>746</sup> Unzulässige Umgehungswerkzeuge i.S.v. Art. 69a Abs. 1 lit. b i.V.m. Art. 39a Abs. 3 URG liegen vor, wenn diese Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Massnahmen sind und abgesehen von der Umgehung nur einen begrenzten wirtschaftlichen Zweck oder Nutzen aufweisen, oder hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Massnahmen zu ermöglichen oder zu erleichtern.<sup>747</sup> Im Unterschied zur Umgehungshandlung selbst ist das Anbieten von Umgehungswerkzeugen sowie das Erbringen von Dienstleistungen zur Umgehung wirksamer technischen Massnahmen auch im Rahmen des Eigengebrauchs unzulässig.<sup>748</sup>

Gemäss dem Wortlaut von Art. 69a Abs. 1 lit. b URG wird eine Verletzung der Norm auf Antrag der verletzten Person mit Busse bestraft. Die Ausgestaltung der Norm als Antragsdelikt führt zu praktischen Schwierigkeiten,

---

<sup>745</sup> DAVID, SHK URG, Art. 69a N 9; BARRELET/EGLOFF, Art. 69a N 7; REHBINDER/VIGANÒ, Art. 69a N 8; SCHWARZENEGGER, ZSR 2008 II, 464.

<sup>746</sup> DAVID, SHK URG, Art. 69a N 9.

<sup>747</sup> AUF DER MAUR, SHK URG, Art. 39a N 10 und DAVID, SHK URG, Art. 69a N 10; RUBLI, Rz. 343 ff.; BARRELET/EGLOFF, Art. 69a N 7; REHBINDER/VIGANÒ, Art. 39a N 18 ff. und Art. 69a N 8.

<sup>748</sup> DAVID, SHK URG, Art. 69a N 11; REHBINDER/VIGANÒ, Art. 69a N 8.

weil die Rechteinhaber durch das blosses Anbieten oder Bewerben von Umgehungswerkzeugen in ihrem Schutz noch gar nicht verletzt worden sind.<sup>749</sup>

- 313 Im Ergebnis ist deshalb festzuhalten, dass entsprechende Umgehungswerkzeuge weder als *Download* noch als *serverbasierte* Online-Anwendung auf einem *Server* in der Schweiz angeboten werden dürfen. Auch die Verbreitung entsprechender Software-Programme über *Filesharing*-Netzwerke ist vom Verbot erfasst. Einige Autoren gehen sogar von einem weitgefassten Werbeverbot aus, welches selbst redaktionelle Beiträge umfasst, bei denen nicht mehr der Informationszweck, sondern die Anpreisung, Empfehlung oder das Auffinden von Umgehungswerkzeugen im Vordergrund steht.<sup>750</sup>

### **b) Strafbarkeit nach StGB**

- 314 Nach Art. 150<sup>bis</sup> StGB wird auf Antrag mit Busse bestraft, wer Decodiergeräte, deren Bestandteile oder Datenverarbeitungsprogramme, die zur unbefugten Entschlüsselung codierter Rundfunkprogramme oder Fernmeldedienste bestimmt und geeignet sind, herstellt, einführt, ausführt, durchführt, in Verkehr bringt oder installiert.<sup>751</sup>
- 315 Ein Dienst ist dann codiert, wenn das ausgesendete Signal bzw. die übermittelten Daten so beschaffen sind, dass sie nur durch einen spezifischen Decodiervorgang verständlich (d.h. für die menschlichen Sinne wahrnehmbar) gemacht werden können.<sup>752</sup> Es handelt sich somit um eine Zugangskontrolle beim Empfänger. Dabei dient die Codierung der Durchsetzung der vom Dienstanbieter getroffenen „Selektion derjenigen Personen, die den Dienst nutzen können“<sup>753</sup>. Nicht erfasst sind Daten, die unverschlüsselt übertragen

---

<sup>749</sup> DAVID, SHK URG, Art. 69a N 9; BARRELET/EGLOFF, Art. 69a N 3; REHBINDER/VIGANÒ, Art. 69a N 2, m.w.H.; SCHWARZENEGGER, ZSR 2008 II, 464, der deshalb auch von einem abstrakten Gefährdungsdeldikt spricht.

<sup>750</sup> AUF DER MAUR, SHK URG, Art. 39a N 13; REHBINDER/VIGANÒ, Art. 39a N 23 und Art. 69a N 8; Vorsicht ist daher geboten, wenn etwa am Ende des Artikels ein entsprechender Hyperlink angebracht wird, welcher das Auffinden des Umgehungswerkzeugs wesentlich erleichtert.

<sup>751</sup> FIOLKA, BSK StGB II, Art. 150<sup>bis</sup> N 28 ff.; STRATENWERTH/WOHLERS, Art. 150<sup>bis</sup> N 1; STRATENWERTH/JENNY/BOMMER, § 16 N 57 f.

<sup>752</sup> FIOLKA, BSK StGB II, Art. 150<sup>bis</sup> N 20, m.w.H.; DONATSCH, Strafrecht III, 269 f.; TRECHSEL/CRAMERI, PK StGB, Art. 150<sup>bis</sup> N 1.

<sup>753</sup> FIOLKA, BSK StGB II, Art. 150<sup>bis</sup> N 20.



werden, auch wenn der Zugang zu diesen Daten spezifisch gesichert ist (Zugangskontrolle beim Anbieter).<sup>754</sup>

Die Entschlüsselung ist dadurch charakterisiert, dass die verschlüsselt aus- 316  
gesendeten Daten wieder in eine für die menschlichen Sinne wahrnehmbare  
Form gebracht werden, wobei den technischen Einzelheiten des Vorgangs  
keine Relevanz zukommt.<sup>755</sup> Das Kriterium der Unbefugtheit ist erfüllt,  
wenn die Entschlüsselung der codierten Angebote nicht durch eine Erlaubnis  
des Anbieters abgedeckt ist.<sup>756</sup> Das Tatbestandsmerkmal der Eignung zur  
unbefugten Entschlüsselung ist erfüllt, wenn Geräte, deren Bestandteile oder  
Datenverarbeitungsprogramme in der Lage sind, codierte Programme zu  
entschlüsseln, ohne hierfür eine Decodiererlaubnis einholen zu müssen.<sup>757</sup>  
Die Bestimmung zur unbefugten Entschlüsselung liegt vor, wenn die Ent-  
schlüsselung als zentrale Zwecksetzung des Geräts oder Geräteteils bzw. des  
Datenverarbeitungsprogramms erscheint.<sup>758</sup>

Gemäss der Botschaft zum revidierten Fernmeldegesetz bezweckt Art. 150<sup>bis</sup> 317  
StGB den Schutz des Vermögens, weshalb diese Bestimmung im Vermö-  
gensstrafrecht anzusiedeln sei.<sup>759</sup> Weiter stellt der Vorfeldtatbestand von  
Art. 150<sup>bis</sup> StGB ein abstraktes Gefährdungsdelikt dar, weil durch das Her-  
stellen, Einführen oder Installieren unautorisierter Decodiergeräte nicht un-  
mittelbar in das Vermögen des Diensteanbieters eingegriffen, sondern dieses  
lediglich gefährdet wird.<sup>760</sup>

Art. 150<sup>bis</sup> StGB ist als Antragsdelikt ausgestaltet. Antragsberechtigt sind 318  
sämtliche Anbieter codierter Rundfunkprogramme und Fernmeldedienste, zu

---

<sup>754</sup> FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 20; STRATENWERTH/JENNY/BOMMER, § 16 N 57.

<sup>755</sup> FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 24.

<sup>756</sup> FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 25.

<sup>757</sup> FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 26; STRATENWERTH/JENNY/BOMMER, § 16 N 59;  
eine sog. Set-Top-Box ist für sich alleine nicht zur Decodierung geeignet, weil diese nur  
den Empfang digitaler TV-Programme ermöglicht, wenn für den Empfang der ver-  
schlüsselten Daten zusätzlich noch eine Smart-Card eingesetzt wird oder die Pro-  
grammcodes sonst wie auf das Gerät geladen werden können; Vgl. auch BGE 139 IV 1,  
Erw. 2., m.H. zum sog. „Cardsharing“.

<sup>758</sup> FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 27; BGE 114 IV 112, Erw. 2 c).

<sup>759</sup> Botschaft FMG 1996, 1452; a.A. FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 13, der einwendet,  
dass dies nur zutreffend sei, falls der Zugang zu den geschützten Diensten einzig gegen  
Zahlung einer Gebühr ermöglicht wird, nicht aber wenn andere Zugangsbeschränkun-  
gen durch Codierung durchgesetzt werden sollen. Dem Wortlaut nach seien aber solche  
Fälle ebenfalls mitumfasst.

<sup>760</sup> FIOKA, BSK StGB II, Art. 150<sup>bis</sup> N 13; DONATSCH, Strafrecht III, 270.

deren Entschlüsselung die entsprechenden Geräte, deren Bestandteile oder Datenverarbeitungsprogramme bestimmt und geeignet sind.<sup>761</sup>

- 319 Im Gegensatz zu codierten Rundfunkprogrammen oder Fernmeldediensten, die nur mit entsprechenden Decodierungsgeräten (Set-Top-Box, Smart-Card etc.) empfangen werden können, wird durch den Kopierschutz im Rahmen des *protected streaming* nicht der unbefugte Empfang durch Unberechtigte verhindert, sondern lediglich die Werknutzung eingeschränkt, (indem die Herstellung dauerhafter Werkkopien verhindert wird). Folglich ist der objektive Tatbestand von Art. 150<sup>bis</sup> StGB in der vorliegenden Sachverhaltskonstruktion nicht erfüllt.

---

<sup>761</sup> RIEDO, 179 f.; CORBOZ, Art. 150<sup>bis</sup> N 11.

## 4. Teil: Sonderfall *P2P-Streaming*

Auch die *Filesharing-Community* hat die Streaming-Technologie für sich 320 entdeckt. Dabei sind (illegale) *P2P-Streaming-Dienste* entstanden, die mit einem attraktiveren Angebot an Filmen und Serien aufwarten als manche (legalen) kostenpflichtigen Streaming-Dienste.<sup>762</sup> Die dazu benötigte Software wird über das Internet u.a. auf bestimmten Webseiten zum *Download* angeboten. Die Distribution der Inhalte erfolgt über ein *BitTorrent*-Netzwerk.<sup>763</sup> Sobald der Nutzer einen gewünschten Filmtitel ausgewählt hat, wird dieser via *BitTorrent*-Protokoll auf den Nutzerrechner heruntergeladen. Im Unterschied zum *Server-Streaming* werden die einzelnen Datenblöcke von den Nutzern nicht nur heruntergeladen, sondern unmittelbar danach an andere Nutzer innerhalb des Netzwerks (*Swarm*) hochgeladen.<sup>764</sup>

Neben den Nutzern als mögliche Urheberrechtsverletzer ist sodann die urheberstrafrechtliche Verantwortlichkeit der übrigen Beteiligten zu prüfen. Hier- 321 zu zählen nebst den Herstellern bzw. Anbietern der Software auch die *Hosting-Provider* der Webseiten, auf denen die Software heruntergeladen werden kann sowie allfällig involvierte Verschlüsselungsdienste, welche damit werben, einen anonymisierten Datenaustausch zwischen den einzelnen Nutzern zu ermöglichen.<sup>765</sup>

---

<sup>762</sup> Siehe dazu etwa <<https://www.cuevana2.tv>>, <<https://popcorn-time.to>>, <<http://popcorn-time.se>> (alle besucht 11. Februar 2018).

<sup>763</sup> S.o. Rz. 29 ff.

<sup>764</sup> Vgl. KUROSE/ROSS, 647; VON GERLACH, 67; das *P2P-Streaming* ist vergleichbar mit dem *P2P-Filesharing* über herkömmliche Tauschbörsen, bei denen die Nutzer untereinander Dateien austauschen, vgl. dazu auch SCHWARZENEGGER, ZSR 2008 II, 442 f.; ders., P2P-Netzwerke, 211 ff.; GLARNER, Musikpiraterie im Internet, 129.

<sup>765</sup> Bspw. hatte der VPN-Anbieter *Kebrum* auf der Webseite [www.time4popcorn.eu](http://www.time4popcorn.eu) (wurde in der Zwischenzeit entfernt) damit geworben, den gesamten Datenverkehr beim *P2P-Streaming* über seine *Server* zu verschlüsseln; siehe dazu SOBIRAJ, <<https://tarnkappe.info/popcorn-time-dominiert-den-markt-bittorrent-als-streaming-getarnt>> (besucht 25. August 2015); auf der Webseite von [popcorn-time.se](http://popcorn-time.se) wird damit geworben, dass die Software über einen eingebauten *VPN-Client* verfügt, um eine anonyme Nutzung des Dienstes zu ermöglichen, siehe <<http://popcorn-time.se>> (besucht 25. August 2015); vgl. auch SCHWARZENEGGER, P2P-Netzwerke, 214, welcher die *P2P-Filesharing-Software* als Bindeglied zwischen Anbieter und *Downloader* bezeichnet, „mit deren Aktivierung durch unzählige User sich das *P2P-Netzwerk* erst konfiguriert“.

## **I. Rechtliche Bewertung des *P2P-Streaming* aus Sicht der Nutzer**

322 Im Unterschied zum *Server-Streaming*<sup>766</sup> agieren die Nutzer beim *P2P-Streaming* sowohl als *Downloader* (*Leecher*) wie auch als *Uploader* (*Seeder*), da die zuvor heruntergeladenen Dateifragmente (*Chunks*) automatisch an andere Nutzer – innerhalb des *P2P-Netzwerks* – hochgeladen werden.<sup>767</sup> Mit Blick auf die technischen Besonderheiten des *P2P-Streaming* werden sogleich die einzelnen Vorgänge aus urheberstrafrechtlicher Perspektive eingehend untersucht. Als einschlägige Tatbestände kommen das unerlaubte Zugänglichmachen von Werken (Art. 67 Abs. 1 lit. g<sup>bis</sup> URG) sowie die unerlaubte Herstellung von Werkexemplaren (Art. 67 Abs. 1 lit. e URG) in Betracht.<sup>768</sup>

### **1. Unerlaubte Zugänglichmachung eines Werks<sup>769</sup>**

#### **A. Objektiver Tatbestand**

323 Als Täter kommt jede beliebige Person in Betracht, die – ohne Einwilligung der Rechteinhaber – ein urheberrechtlich geschütztes Werk mit irgendwel-

---

<sup>766</sup> S.o. Rz. 26 f.

<sup>767</sup> KUROSE/ROSS, 647; VON GERLACH, 67.

<sup>768</sup> Ebenfalls denkbar ist eine Verletzung von verwandten Schutzrechten nach Art. 69 URG. Da die einzelnen Tatbestände von Art. 69 URG analog zur denjenigen von Art. 67 URG aufgebaut sind, wird nachfolgend auf eine gesonderte Darstellung verzichtet; siehe zu dieser Thematik auch DAVID, SHK URG, Art. 69 N 3a; BARRELET/EGLOFF, Art. 69 N 1; SCHWARZENEGGER, P2P-Netzwerke, 215 f.; GLARNER, Musikpiraterie im Internet, 90 ff.

<sup>769</sup> Vor der Einführung des Tatbestandes der unerlaubten Zugänglichmachung (Art. 67 Abs. 1 lit. g<sup>bis</sup> URG) wurde in Fällen des *P2P-Filesharings* u.a. eine Strafbarkeit wegen unerlaubter Verbreitung von Werkexemplaren (Art. 67 Abs. 1 lit. f URG) geprüft. Umstritten war dabei, ob die Bestimmung bloss materialisierte Werkexemplare umfassen würde oder ob auch digitale Werke erfasst würden. Zudem war strittig, ob der Wortlaut der Bestimmung auch unkörperliche Verbreitungsformen umfasst. Mit der Einführung von Art. 67 Abs. 1 lit. g<sup>bis</sup> URG hat dieser Meinungsstreit an Aktualität verloren, da von diesem Tatbestand gerade jene Fallkonstellationen erfasst werden, in denen unkörperliche Werke „on-demand“ über das Internet zugänglich gemacht werden. Vgl. DAVID, SHK URG, Art. 67 N 13; SCHWARZENEGGER, P2P-Netzwerke, 216 ff.; GLARNER, Musikpiraterie im Internet, 102 ff.

chen Mitteln so zugänglich macht, dass Personen von Orten und zu Zeiten ihrer Wahl darauf zugreifen können.<sup>770</sup>

Eine Besonderheit beim *P2P-Streaming* liegt darin, dass der einzelne Nutzer 324 (bestenfalls) am Ende des Wiedergabevorganges über das gesamte Werk verfügt. Zuvor besitzt er nur Bruchstücke des Werks und kann folglich auch nur diese öffentlich zugänglich machen.<sup>771</sup> Bei den einzelnen ausgetauschten Werkfragmenten (*Chunks*) ist zudem fraglich, ob diese bereits die von Art. 2 Abs. 1 URG geforderte Schöpfungshöhe erreichen.<sup>772</sup> Um dieser Problematik bei *P2P-Netzwerken* beizukommen, wird deshalb vorgeschlagen, dass der Tatbestand der unerlaubten Zugänglichmachung bereits dann bejaht werden müsse, wenn sich aus der „Gesamtheit der in Umlauf befindlichen Dateifragmente eine abspielbare Kopie des Werks ergibt“<sup>773</sup>. Übertragen auf die Situation beim *P2P-Streaming* muss für den Nachweis der unerlaubten Zugänglichmachung i.S.v. Art. 10 Abs. 2 lit. c URG genügen, wenn für die am *P2P-Streaming* beteiligten Nutzer die Wiedergabe des Werks bzw. von (schutzfähigen) Teilen davon möglich ist.

Entscheidend ist demnach nicht, ob bei isolierter Betrachtung die durch den 325 einzelnen Nutzer zugänglich gemachten Dateifragmente als unerlaubte Zugänglichmachung eines Werks zu qualifizieren sind, sondern ob die Gesamtheit der am *P2P-Streaming-Netzwerk* beteiligten Nutzer – durch gemeinschaftliche Tatbegehung – den Tatbestand von Art. 67 Abs. 1 lit. g<sup>bis</sup> URG erfüllen. Die Tathandlung besteht im gemeinschaftlichen unerlaubten Zugänglichmachen von urheberrechtlich geschützten Werkdaten an andere Nut-

---

<sup>770</sup> DAVID, SHK URG, Art. 67 N 20, mit dem Hinweis, dass darunter die sog. „on-demand“-Angebote zu verstehen seien; REHBINDER/VIGANÒ, Art. 67 N 14, m.H. auf *P2P-Netzwerke*.

<sup>771</sup> HEINEMEYER/KREITLOW/NORDMEYER/SABELLEK, ZUM 2012, 283, weisen darauf hin, dass der Datenaustausch in einer Netzwerkstruktur vonstatten geht, in welcher eine Vielzahl beteiligter Nutzer untereinander kleinste Datenblöcke austauschen.

<sup>772</sup> HEINEMEYER/KREITLOW/NORDMEYER/SABELLEK, ZUM 2012, 281, vergleichen den Versuch, eine Datei aus Chunks zusammenzusetzen mit dem Bestreben, geschnitzelte Leber in ihren Ursprungszustand zurückzusetzen – wobei die einzelnen Datenblöcke nicht einmal vollständig vorhanden sein müssen.

<sup>773</sup> HEINEMEYER/KREITLOW/NORDMEYER/SABELLEK, ZUM 2012, 282, wobei sich die Autoren bei ihren Ausführungen auf eine herkömmliche *P2P-Filesharing-Plattform* beziehen, bei welchem das Werk vorab auf ein Speichermedium auf dem Nutzerrechner heruntergeladen werden muss und erst im Anschluss konsumiert werden kann.

zer innerhalb eines *P2P-Netzwerks*.<sup>774</sup> Damit der Datenaustausch mittels *P2P-Streaming* reibungslos funktioniert, ist die Beteiligung einer möglichst grossen Zahl von Nutzern erforderlich. Durch seine Teilnahme am *P2P-Streaming* leistet jeder einzelne *Uploader* einen wesentlichen (auch wenn nicht unbedingt unerlässlichen) Beitrag für den illegalen Datenaustausch.<sup>775</sup>

- 326 Der Datenaustausch beim *P2P-Streaming* zwischen den am Netzwerk beteiligten Nutzern läuft automatisiert ab und stellt keine Werkverwendung im persönlichen Bereich bzw. im Kreis von Personen, die unter sich eng verbunden sind, dar.<sup>776</sup> Eine Berufung auf die in Art. 19 Abs. 1 lit. a URG verankerte Schrankenregelung zum Privatgebrauch ist folglich ausgeschlossen. Soweit keine Einwilligung der Rechteinhaber hinsichtlich des *P2P-Streaming* vorliegt, erfüllen die am *P2P-Streaming* beteiligten Nutzer den objektiven Tatbestand von Art. 67 Abs. 1 lit. g<sup>bis</sup> URG in Mittäterschaft.

## B. Subjektiver Tatbestand

- 327 Die Mittäterschaft setzt in subjektiver Hinsicht einen gemeinsamen Tatentschluss voraus, wobei dieser auch konkludent zum Ausdruck gebracht werden kann.<sup>777</sup> Der Mittäter kann sich seinen Tatentschluss auch erst sukzessive zu eigen machen, falls er bei der Planung und Entschlussfassung nicht direkt beteiligt war.<sup>778</sup>
- 328 In den Medien wurde bereits ausführlich über das Phänomen und die Funktionsweise der *P2P-Streaming-Dienste* berichtet. Auf den Webseiten, über welche die *P2P-Streaming-Software* heruntergeladen werden kann, ist zudem meist auch ein Hinweis angebracht, dass die Filme und TV-Serien über einen sog. *Torrent* geladen werden.<sup>779</sup> Die Nutzer haben daher in aller Regel zumindest eine laienhafte Vorstellung, dass bei Verwendung einer *P2P-Streaming-Software* die urheberrechtlich geschützten Werke nicht bloss heruntergeladen, sondern zugleich auch anderen Nutzern innerhalb des *P2P-Netzwerks* unerlaubt zugänglich gemacht werden. Wer im Wissen um diese

---

<sup>774</sup> Die *Upload*-Funktion kann bei der *P2P-Streaming-Software* normalerweise nicht deaktiviert werden. Vgl. HEINEMEYER/KREITLOW/NORDMEYER/SABELLEK, ZUM 2012, 283.

<sup>775</sup> Vgl. DONATSCH/TAG, 180, m.w.H.

<sup>776</sup> Vgl. SCHWARZENEGGER, P2P-Netzwerke, 219.

<sup>777</sup> BGE 126 IV 84, Erw. 2c/aa; 125 IV 134, Erw. 3a; 118 IV 227, Erw. 5d/aa.

<sup>778</sup> FORSTER, BSK StGB I, N 12 Vorb. Art. 24; DONATSCH/TAG, 178.

<sup>779</sup> Vgl. <<https://popcorn-time.to>> oder <<http://popcorn-time.se>> (beide besucht 11. Februar 2018).

Vorgänge über ein *P2P-Netzwerk* urheberrechtlich geschützte Werke unbekannten Dritten zugänglich macht, nimmt zumindest in Kauf, objektiv tatbestandsmässig zu handeln.<sup>780</sup>

### C. Rechtswidrigkeit und Schuld

Es sind in der vorliegenden Konstellation kaum Anwendungsfälle der gesetzlichen oder übergesetzlichen Rechtfertigungsgründe denkbar. Ein Rechtsirrtum nach Art. 21 StGB wird i.d.R. deshalb ausgeschlossen sein, weil die Nutzer bei Aufwendung der gebotenen Sorgfalt die Rechtswidrigkeit ihres Tuns hätten erkennen können.<sup>781</sup>

## 2. Unerlaubte Herstellung von Werkexemplaren

### A. Objektiver Tatbestand

Als Täter einer unerlaubten Herstellung von Werkexemplaren i.S.v. Art. 67 Abs. 1 lit. e URG kommt jede Person in Betracht, die ohne Zustimmung der Rechteinhaber urheberrechtlich geschützte Werke vervielfältigt. Der *Download* aus dem Internet stellt eine solche Vervielfältigungshandlung dar.<sup>782</sup>

Beim *P2P-Streaming* werden kontinuierlich das gesamte Werk bzw. Teile davon auf ein Speichermedium im Nutzerrechner heruntergeladen. Die auf dem Datenträger fixierten Werkdaten stellen ein Werkexemplar dar.<sup>783</sup> Da die Herstellung der Werkvervielfältigung im Rahmen des *P2P-Streaming* zumeist ohne die Einwilligung der Rechteinhaber erfolgt, ist das objektive Tatbestandsmerkmal der Unrechtmässigkeit in aller Regel erfüllt.<sup>784</sup>

Das Vorliegen einer bloss vorübergehenden Vervielfältigung i.S.v. Art. 24a URG ist zu verneinen, da die temporäre Werkkopie im Nutzerrechner nicht bloss der Wiedergabe des Werks dient, sondern hauptsächlich zum Zweck

---

<sup>780</sup> SCHWARZENEGGER, P2P-Netzwerke, 222 f.

<sup>781</sup> SCHWARZENEGGER, P2P-Netzwerke, 223.

<sup>782</sup> PFORTMÜLLER, SHK URG, Art. 10 N 5; BARRELET/EGLOFF, Art. 10 N 12; SCHWARZENEGGER, P2P-Netzwerke, 225, der darauf hinweist, dass es dabei unbeachtlich ist, wenn die Kopie „aus mehreren Teilen zusammengesetzt und von verschiedenen Quellen heruntergeladen wird“; NEFF/ARN, SIWR II/2, 227.

<sup>783</sup> DAVID, SHK URG, Art. 67 N 13; SCHWARZENEGGER, P2P-Netzwerke, 225.

<sup>784</sup> SCHWARZENEGGER, P2P-Netzwerke, 226, GLARNER, Musikpiraterie im Internet, 76 ff.

des *Filesharing* innerhalb des *P2P-Netzwerks* hergestellt wird.<sup>785</sup> Auch die Schrankenregelung zum Privatgebrauch nach Art. 19 Abs. 1 lit. a URG ist in der vorliegenden Konstellation nicht anwendbar. Die auf den Nutzerrechner heruntergeladene Werkkopie wird nicht bloss vom Nutzer selbst bzw. einem Kreis von unter sich eng verbundenen Personen wie Verwandte oder Freunde verwendet, sondern darüber hinaus automatisch einer unbestimmten Vielzahl beliebiger Personen mittels *P2P-Streaming-Software* zugänglich gemacht.<sup>786</sup>

## **B. Subjektiver Tatbestand**

- 333 Der subjektive Tatbestand von Art. 67 Abs. 1 lit. e URG setzt voraus, dass der Täter mit Vorsatz handelt, wobei Eventualvorsatz genügt.<sup>787</sup> Durch die Teilnahme am *P2P-Streaming-Netzwerk* nehmen die Nutzer zumindest in Kauf, dass auf ihren Rechnern unerlaubte Vervielfältigungen von urheberrechtlich geschützten Werken hergestellt werden.

## **C. Rechtswidrigkeit und Schuld**

- 334 Es sind kaum gesetzliche oder übergesetzliche Rechtfertigungsgründe denkbar. Ein Rechtsirrtum nach Art. 21 StGB wird i.d.R. ausgeschlossen sein, da die Nutzer bei Aufwendung der gebotenen Sorgfalt die Rechtswidrigkeit ihres Tuns hätten erkennen können.<sup>788</sup>

---

<sup>785</sup> S.o. Rz. 29 ff.

<sup>786</sup> SCHWARZENEGGER, P2P-Netzwerke, 228, mit dem Hinweis, dass ein zustimmungsfreier rechtmässiger Eigengebrauch nach Art. 19 Abs. 1 lit. a URG nur dann angenommen werden könne, wenn die *Upload-Funktion* des *P2P-Sharing-Programms* völlig blockiert ist. Die *P2P-Streaming-Apps* sehen eine solche Möglichkeit zumeist nicht vor.

<sup>787</sup> BARRELET/EGLOFF, Art. 67 N 6a.

<sup>788</sup> SCHWARZENEGGER, P2P-Netzwerke, 230.



## II. Rechtliche Bewertung des *P2P-Streaming* aus Sicht der übrigen Beteiligten

### 1. Strafbarkeit der Anbieter der *P2P-Streaming-Software*

Nachfolgend wird untersucht, inwieweit das Anbieten einer Software zum Zwecke des *P2P-Streaming* von urheberrechtlich geschützten Werken – ohne Einwilligung der Rechteinhaber – strafrechtlich relevant ist.<sup>789</sup>

Berechtigt zur Stellung eines Strafantrags sind die in ihren Rechten verletzten Personen. Darunter fallen sämtliche Rechteinhaber von Werken, die über die *P2P-Streaming-Software* angeboten werden. Falls die *P2P-Streaming-Software* kommerziell betrieben wird (etwa durch Werbefinanzierung) und hierdurch regelmässige Einnahmen erzielt werden, die einen namhaften Beitrag an die Lebensgestaltung der Anbieter der Software darstellen, liegt eine gewerbsmässige Urheberrechtsverletzung vor, die von Amtes wegen zu verfolgen ist.<sup>790</sup>

#### A. Unerlaubte Zugänglichmachung des Werks

##### a) *Alleintäterschaft*

Da die Anbieter der *P2P-Streaming-Software* für gewöhnlich selbst keine urheberrechtlich geschützten Inhalte auf die Rechner der Nutzer oder auf den Server eines *Filehosters* hochladen, ist eine Alleintäterschaft ausgeschlossen.<sup>791</sup> Der Tatbeitrag der Software-Anbieter beschränkt sich auf das Zurver-

---

<sup>789</sup> Zum räumlichen Geltungsbereich des Schweizer Urheberrechts vgl. Rz. 37.

<sup>790</sup> In der Praxis sollten keine zu hohen Anforderungen an die Annahme einer gewerbsmässigen Tatbegehung gestellt werden. Der Umfang der so erzielten Einnahmen lässt sich ohnehin erst im Laufe des Verfahrens bestimmen. Liegen entsprechende Hinweise auf eine urheberrechtswidrige, werbefinanzierte *P2P-Streaming-Software* vor, sollten die Strafverfolgungsbehörden ihre Ermittlungen gegen die Anbieter der Software aufnehmen können, ohne dass es hierfür eines gesonderten Strafantrags bedarf.

<sup>791</sup> Die Dienstbetreiber von Popcorn Time „ziehen sich auf den Standpunkt zurück, selbst keine Inhalte zu verteilen“, vgl. STEIER, Popcorn Time, <<http://www.nzz.ch/digital/popcorn-time-peer-to-peer-bittorrent-1.18506299>> (besucht 25. August 2015),

fügungstellen und den Unterhalt einer *P2P-Streaming-Software*.<sup>792</sup> Die verfügbaren Inhalte samt den dazugehörigen *Locator*-Dateien (*.torrent*-Dateien) werden darin übersichtlich und geordnet dargestellt. Die Software ermöglicht das Streaming der Inhalte über ein *P2P-Netzwerk*.<sup>793</sup> Dabei werden die Inhalte zwischen den am Netzwerk beteiligten Nutzern (*Peers*) ausgetauscht. Da der *Upload* der geschützten Inhalte auf die Rechner der anderen Nutzer (*Peers*) nicht unmittelbar durch die Anbieter der *P2P-Streaming-Software*, sondern durch die Nutzer selbst ausgelöst wird, ist eine unerlaubte Zugänglichmachung i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG durch die Anbieter in Alleintäterschaft zu verneinen.<sup>794</sup>

### **b) Mittelbare Täterschaft**

- 338 Bei der mittelbaren Täterschaft missbraucht der Täter den Tatmittler als „willenloses“ oder zumindest nicht vorsätzlich handelndes Instrument der Tatausführung.<sup>795</sup> Diese Konstellation ist mit Blick auf das Anbieten der *P2P-Streaming-Software* abzulehnen. Die Nutzer werden u.a. durch einen Hinweis auf der Webseite darauf aufmerksam gemacht, dass die gestreamten Inhalte nicht bloss herunter- sondern auch hochgeladen werden. Zudem wurde über die Funktionsweise der *P2P-Streaming-Software* sowohl im Internet als auch in der Tagespresse und in Fachzeitschriften bereits ausführlich berichtet.<sup>796</sup> Ein Sachverhaltsirrtum scheint deshalb ausgeschlossen. Auch werden die Nutzer in keiner Weise dazu genötigt, das Programm zu nutzen. Die Teilnahme erfolgt vielmehr in Eigenverantwortung der Nutzer sowie im Wissen darüber, dass bei der Verwendung einer *P2P-Streaming-Software* geschützte Inhalte an andere Nutzer hochgeladen werden.

---

<sup>792</sup> Künftig sollen auch Updates via *P2P-Technologie* verteilt werden, siehe GREENBERG, <<http://www.wired.com/2015/03/inside-popcorn-time-piracy-party-hollywood-cant-stop>> (besucht 25. August 2015).

<sup>793</sup> KUROSE/ROSS, 172 ff.

<sup>794</sup> DAVID, SHK URG, Art. 67 N 21; zur Rechtslage in Deutschland REINBACHER, NStZ 2014, 58.

<sup>795</sup> FORSTER, BSK StGB I, N 28 Vorb. Art. 24; BGE 120 IV 17, Erw. 2d.

<sup>796</sup> STEIER, Netflix für Piraten, <<http://www.nzz.ch/digital/popcorn-time-yts-github-1.18264598>> oder STÖCKER, <<http://www.spiegel.de/netzwelt/web/streaming-software-popcorn-time-schick-hip-illegal-a-959089.html>> (beide besucht 25. August 2015).

**c) Mittäterschaft**

**aa) Objektiver Tatbestand**

Bei der Prüfung der Mittäterschaft ist das Anbieten der *P2P-Streaming-Software* im Kontext zu den anderen Vorgängen zu betrachten, die letztlich das (illegale) P2P-Streaming ermöglichen. Eine gewöhnliche *P2P-Software*<sup>797</sup> dient dem Datenaustausch zwischen den einzelnen Nutzern. Dabei sind zahlreiche legale Verwendungsmöglichkeiten denkbar.<sup>798</sup> Die *P2P-Streaming-Software* durchsucht demgegenüber aktiv Verzeichnisse von einschlägigen Portalen, auf denen geschützte Werke ohne Einwilligung der Rechteinhaber öffentlich zugänglich gemacht werden. Insoweit ist die Situation vergleichbar mit der Veröffentlichung von *URL-Adressen* oder *Locator-Dateien* (.torrent-Dateien) zu urheberrechtlich geschützten Werken auf Webseiten im Internet.<sup>799</sup> Die *P2P-Streaming-Software* geht allerdings noch einen Schritt weiter, da die heruntergeladenen Inhalte (bzw. Teile davon) automatisch an andere Nutzer hochgeladen werden. Der *Upload* von geschützten Inhalten an andere Nutzer ist als unerlaubte Zugänglichmachung eines Werks i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG zu qualifizieren. Die *P2P-Streaming-Software* kann deshalb fast nur zu illegalen Zwecken verwendet werden. 339

Das öffentliche Anbieten einer *P2P-Streaming-Software*, die auf den illegalen Austausch von urheberrechtlich geschützten Inhalten zwischen den Nutzern ausgelegt ist, könnte als unerlaubtes Zugänglichmachen eines Werks in Mittäterschaft qualifiziert werden. Nach Rechtsprechung des Bundesgerichts gilt als Mittäter, „wer bei der Entschliessung, Planung oder Ausführung eines Delikts vorsätzlich und in massgebender Weise mit anderen Tätern zusammenwirkt, so dass er als Hauptbeteiligter dasteht; dabei kommt es darauf an, ob der Tatbeitrag nach den Umständen des konkreten Falles und dem Tatplan für die Ausführung des Deliktes so wesentlich ist, dass sie mit ihm steht oder fällt“<sup>800</sup>. 340

---

<sup>797</sup> Wie etwa BitTorrent, uTorrent, Vuze, eMule oder BitComet.

<sup>798</sup> Etwa der Austausch von nicht urheberrechtlich geschützten Dateien; vgl. auch SCHWARZENEGGER, P2P-Netzwerke, 233 ff.; GLARNER, Musikpiraterie im Internet, 127.

<sup>799</sup> Urteil 6B\_757/2010 des Bundesgerichts vom 7. Februar 2011, Erw. 4; SCHWARZENEGGER, P2P-Netzwerke, 237 ff.

<sup>800</sup> BGE 133 IV 76, Erw. 2.7; 130 IV 58, Erw. 9.2.1; 126 IV 84, Erw. 2 c/aa; 125 IV 134, Erw. 3a; 120 IV 265, Erw. 2c/aa.

- 341 Durch das öffentliche Zurverfügungstellen einer *P2P-Streaming-Software* wirken die Anbieter in massgebender Weise an der Begehung der Urheberrechtsverletzungen mit. Ohne die angebotene *P2P-Streaming-Software* wäre der illegale Datenaustausch unter den Nutzern (Peers) im Rahmen des *P2P-Streaming* nicht denkbar.<sup>801</sup> In der Phase der Entschlussfassung und der Planung sind die Anbieter der Software massgeblich beteiligt. Während der Ausführungsphase, in der von den Nutzern aktiv geschützte Inhalte bzw. Teile davon an Dritte hochgeladen werden, üben die Anbieter weiterhin einen tragenden Einfluss aus, indem sie um den Unterhalt der Software besorgt sind und diese regelmässig aktualisieren, die Auswahl der Inhalte treffen und dafür sorgen, dass diese übersichtlich präsentiert werden.<sup>802</sup>

*bb) Subjektiver Tatbestand*

- 342 In subjektiver Hinsicht setzt die Mittäterschaft einen gemeinsamen Tatentschluss voraus.<sup>803</sup> Dabei genügt es, wenn dieser konkludent zum Ausdruck gelangt.<sup>804</sup> Auch braucht der Mittäter an der ursprünglichen Entschlussfassung nicht von Anfang an mitgewirkt zu haben – er kann sich den Tatentschluss auch erst sukzessive zu eigen machen.<sup>805</sup>
- 343 Im Unterschied zu herkömmlichen Tauschbörsen wird die *P2P-Streaming-Software* nahezu ausschliesslich dazu verwendet um illegales *Filesharing* zu betreiben. Indem die Anbieter die *P2P-Streaming-Software* zum Download für die Nutzer bereithalten, bringen diese zumindest konkludent zum Ausdruck, dass sie einer Urheberrechtsverletzung durch unerlaubtes Zugänglichmachen eines Werks i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG, Vorschub leisten wollen. Durch das Aktualisieren, Bewerben und Unterhalten der *P2P-Streaming-Software* manifestiert sich der Wille der Anbieter zur Teilnahme an den mittels *P2P-Streaming* begangenen Urheberrechtsverletzungen.

---

<sup>801</sup> SCHWARZENEGGER, P2P-Netzwerke, 232, mit dem Hinweis, dass der konkrete objektive Kausalzusammenhang nicht unterbrochen wird, durch den Einwand dass die Nutzer auch ein alternatives *P2P-Programm* hätten einsetzen können.

<sup>802</sup> Dies auch im Unterschied zu den *Filehostern*, die lediglich Speicherkapazitäten für ihre Nutzer zur Verfügung stellen.

<sup>803</sup> FORSTER, BSK StGB I, N 12 Vorb. Art. zu 24.

<sup>804</sup> BGE 126 IV 84, Erw. 2c/aa; 125 IV 134, Erw. 3a; 118 IV 227, Erw. 5d/aa.

<sup>805</sup> FORSTER, BSK StGB I, N 12 Vorb. zu Art. 24; DONATSCH/TAG, 178 f.; BGE 130 IV 58, Erw. 9.2.1; 125 IV 134, Erw. 3a.

*cc) Rechtswidrigkeit und Schuld*

Unbeachtlich ist der Umstand, dass die Nutzer teilweise durch einen Warnhinweis auf der Webseite des Anbieters darauf aufmerksam gemacht werden, dass die Software geschützte Inhalte über *Torrents* streamt und dass das Hoch- und Herunterladen geschützter Werke in bestimmten Ländern verboten ist, weshalb die Nutzung auf eigene Gefahr erfolgt.<sup>806</sup> Das bloße Anbringen eines „Warnhinweises“ befreit die Anbieter von deren Verantwortlichkeit in keiner Weise. Anwendungsfälle der gesetzlichen oder übergesetzlichen Rechtfertigungsgründe sind nicht ersichtlich und auch ein Rechtsirrtum ist mit Blick auf die Handlungen der Anbieter der *P2P-Streaming-Software* ausgeschlossen.<sup>807</sup>

*dd) Gewerbsmässiges Handeln*

Werden durch das Anbieten der *P2P-Streaming-Software* direkt oder indirekt (etwa durch den Verkauf der Software oder durch Werbeeinnahmen) Einkünfte erzielt, die geeignet sind, einen namhaften Teil der Lebenskosten der Anbieter zu decken, liegt eine gewerbsmässige Tatbegehung i.S.v. Art. 67 Abs. 2 URG vor.<sup>808</sup>

*d) Anstiftung*

Eine Anstiftung nach Art. 24 StGB setzt voraus, dass der Anstifter auf den nachmaligen Täter dahingehend einwirkt, dass sich dieser dazu entschliesst, ein Verbrechen oder Vergehen zu verüben und dieses auch tatsächlich begeht. Wer bloss eine Situation schafft, in der sich der Täter zur Begehung einer Straftat entschliessen könnte, erfüllt den objektiven Tatbestand der Anstiftung nicht.<sup>809</sup> Folglich erfüllt das bloße Anbieten einer *P2P-Streaming-Software* den Tatbestand einer Anstiftung zur Begehung von Urheberrechtsverletzungen nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG i.V.m. Art. 24

---

<sup>806</sup> Der *Download* der Software wird nicht etwa durch Geo-Sperren auf jene Länder beschränkt, in denen der *Upload* von urheberrechtlich geschützten Werken zulässig ist; s.o. Rz. 269 ff.

<sup>807</sup> Die Software wird für jedermann im Internet zugänglich gemacht. Die Anbieter nehmen damit zumindest in Kauf, dass die Software auch in Ländern eingesetzt wird, in denen das öffentliche Zugänglichmachen eines geschützten Werks – ohne die Einwilligung der Rechteinhaber – gegen das Urheberrecht verstösst.

<sup>808</sup> BGE 123 IV 113, Erw. 2c.

<sup>809</sup> BGE 128 IV 11, Erw. 2a; BGE 127 IV 122, Erw. 2b/aa; FORSTER, BSK StGB I, Art. 24 N 15; STRATENWERTH, § 13 Rz. 101; GLARNER, Musikpiraterie im Internet, 127.

StGB nicht, da die Anbieter lediglich ermöglichen, urheberrechtlich geschützte Werke über das Internet auf dem Wege des *P2P-Streaming* auszutauschen.

**e) Gehilfenschaft**

**aa) Objektiver Tatbestand**

- 347 Wird – entgegen der hier vertretenen Ansicht – eine Mittäterschaft abgelehnt, ist sodann die Gehilfenschaft zu einem unerlaubten Zugänglichmachen von Werken zu prüfen (Art. 67 Abs. 1 lit. g<sup>bis</sup> URG i.V.m. Art. 25 StGB). Der Gehilfe will durch seine Hilfeleistung die Haupttat fördern und nimmt zumindest in Kauf, dadurch die Begehung einer Straftat zu erleichtern.<sup>810</sup> Bei der Gehilfenschaft ist der Tatbeitrag des Gehilfen bloss von untergeordneter Natur und für die Verwirklichung der Straftat nicht derart wesentlich, dass diese mit der Hilfeleistung „steht oder fällt“.<sup>811</sup>
- 348 In einem Entscheid aus dem Jahre 2011 hatte das Bundesgericht zu beurteilen, ob das öffentliche Anbieten sog. *Hash-Links*<sup>812</sup> zu *Filesharing*-Angeboten gegen das Urheberrecht verstösst.<sup>813</sup> Ein *Hash-Link* dient der automatisierten Suche nach einer bestimmten Datei in einem *P2P-Netzwerk* und letztlich dem Herunterladen derselben.<sup>814</sup> In seinem Verdikt schützte das Bundesgericht den Entscheid der Vorinstanz und verurteilte den Anbieter der *Hash-Links* zu urheberrechtlich geschützten Werken, die innerhalb von *P2P-Netzwerken* zwischen den beteiligten Nutzern ausgetauscht wurden, wegen gewerbsmässiger Gehilfenschaft zur Verletzung von Urheberrechten (Art. 67 Abs. 1 lit. f und lit. g URG i.V.m. Art. 25 StGB).<sup>815</sup>
- 349 Vorliegend ist zu beachten, dass sich der Tatbeitrag der Anbieter nicht bloss auf das Anbieten der *P2P-Streaming-Software* beschränkt. Um die Software einem möglichst breiten Publikum zugänglich zu machen, ist neben dem Unterhalt der Webseite auch eine periodische Aktualisierung und Weiterent-

---

<sup>810</sup> FORSTER, BSK StGB I, Art. 25 N 3.

<sup>811</sup> FORSTER, BSK StGB I, Art. 25 N 3.

<sup>812</sup> Suchhilfen zu Links.

<sup>813</sup> Urteil 6B\_757/2010 des Bundesgerichts vom 7. Februar 2011.

<sup>814</sup> SCHWARZENEGGER, P2P-Netzwerke, 237, m.w.H.

<sup>815</sup> Urteil 6B\_757/2010 des Bundesgerichts vom 7. Februar 2011, Erw. 4.4, „Die rechtliche Würdigung der Vorinstanz zur Teilnahmeform der Gehilfenschaft ist bundesrechtlich nicht zu beanstanden“ (der Sachverhalt bezog sich auf Handlungen, die von 2001 bis März 2004 und damit vor der Revision des URG im Jahre 2008 stattgefunden haben).

wicklung der Software erforderlich. Zudem wird auch das Angebot der verfügbaren Werke (Filme und TV-Serien) laufend erweitert. Bei dieser Gesamtbetrachtung ist das Anbieten als aktive Hilfeleistung zu qualifizieren und ein objektiv kausaler Förderungsbeitrag mit Blick auf die unerlaubte Zugänglichmachung von Werken i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG zu bejahen.

Alternativ könnte der fördernde Tatbeitrag der Anbieter von *P2P-Streaming-Software* auch in der Unterlassung der Einstellung des Anbietens und des Unterhalts der *P2P-Streaming-Software* gesehen werden. Spätestens zu jenem Zeitpunkt, in dem die Software aktiv von den Nutzern heruntergeladen und zum Zwecke des illegalen *P2P-Streaming* eingesetzt wird, müssen die Anbieter davon ausgehen, dass weitere Nutzer die Software herunterladen und Urheberrechtsverletzungen begehen werden.<sup>816</sup> Weil durch das öffentliche Anbieten der *P2P-Streaming-Software* eine nahe und ernsthafte Gefahr der Verletzung von Urheberrechten geschaffen wird, ist m.E. eine Garantenstellung aus Ingerenz zu bejahen.

#### *bb) Subjektiver Tatbestand*

In subjektiver Hinsicht setzt die Gehilfenschaft nach Art. 25 StGB voraus, dass der Täter vorsätzlich Hilfe zu einem Verbrechen oder Vergehen leistet, wobei Eventualvorsatz genügt.<sup>817</sup> Der (Eventual-)Vorsatz des Gehilfen muss sich sowohl auf die Haupttat wie auch auf die Hilfeleistung beziehen.<sup>818</sup>

Strittig ist in dieser Konstellation m.E. einzig, ob der Tatentschluss des Haupttäters im Zeitpunkt des Anbietens der *P2P-Streaming-Software* bereits gefasst worden sein muss.<sup>819</sup> SCHWARZENEGGER führt dazu aus, dass „der Vorsatz beim Gehilfen desto weniger gegeben sein wird, je weiter seine Unterstützung im Vorfeld erfolgt“<sup>820</sup>. Da die *P2P-Streaming-Software* auch in Ländern angeboten wird bzw. heruntergeladen werden kann, die das öffentliche Zugänglichmachen von geschützten Werken ohne Einwilligung der Rechteinhaber unter Strafe stellen, nehmen die Anbieter der Software zumindest in Kauf, dadurch die Begehung von Urheberrechtsverletzungen zu

---

<sup>816</sup> Urteil 6B\_757/2010 des Bundesgerichts vom 7. Februar 2011, Erw. 4.4; SCHWARZENEGGER, P2P-Netzwerke, 243.

<sup>817</sup> BGE 121 IV 109, Erw. 3a; FORSTER, BSK StGB I, Art. 25 N 3.

<sup>818</sup> SCHWARZENEGGER, P2P-Netzwerke, 242 ff.

<sup>819</sup> SCHWARZENEGGER, P2P-Netzwerke, 242 ff., m.w.H.

<sup>820</sup> SCHWARZENEGGER, P2P-Netzwerke, 243.

fördern.<sup>821</sup> Auch war es für die Anbieter zweifellos voraussehbar, dass die *Software* zur Begehung von Urheberrechtsverletzungen genutzt wird.

*cc) Rechtswidrigkeit und Schuld*

- 353 Es sind in der vorliegenden Konstellation weder Rechtfertigungs- noch Schuldausschlussgründe ersichtlich. Da sich die Anbieter der Rechtswidrigkeit ihrer Handlungen bewusst waren bzw. diese bei der Anwendung der gebotenen Sorgfalt hätten erkennen können, ist vorliegend auch ein rechtlich beachtlicher Rechtsirrtum ausgeschlossen.

**B. Unerlaubte Herstellung von Werkexemplaren**

*a) Alleintäterschaft*

- 354 Da die Anbieter der *P2P-Streaming-Software* keine urheberrechtlich geschützten Inhalte auf *Server* bzw. an die am Netzwerk beteiligten Nutzer hochladen, liegt keine unerlaubte Herstellung von Werkexemplaren nach Art. 67 Abs. 1 lit. e URG in Alleintäterschaft vor.<sup>822</sup>

*b) Mittelbare Täterschaft*

- 355 Eine mittelbare Täterschaft ist mit Blick auf den vorliegenden Sachverhalt abzulehnen, da die Nutzer weder dazu genötigt werden, die *P2P-Streaming-Software* zu verwenden, noch werden diese über die mit der Nutzung der Software verbundenen Speichervorgänge auf dem Nutzerrechner zum Zweck des *Filesharing* getäuscht.<sup>823</sup>

*c) Mittäterschaft*

*aa) Objektiver Tatbestand*

- 356 Innerhalb der Phase der Entschlussfassung und Planung kommt den Anbietern der *Software* eine massgebliche Rolle zu. Die Tatherrschaft zeigt sich darin, dass diese darüber bestimmen können, ob die *Software* den Nutzern öffentlich zugänglich gemacht werden soll. Im Ausführungsstadium üben die

---

<sup>821</sup> Entscheidend ist dabei, dass die *P2P-Streaming-Software* fast ausschliesslich zu illegalen Zwecken eingesetzt wird.

<sup>822</sup> S.o. Rz. 337 f.

<sup>823</sup> S.o. Rz. 338.



Anbieter weiterhin einen „tragenden Einfluss“ aus, indem sie für den Unterhalt der Software sorgen und die Auswahl der gestreamten Inhalte festlegen. Weil das *P2P-Streaming* ohne die *Software* nicht funktionieren würde, ist der Tatbeitrag der Anbieter der Software als derart wichtig einzustufen, dass diese als Hauptbeteiligte erscheinen.<sup>824</sup>

*bb) Subjektiver Tatbestand*

Im öffentlichen Anbieten der *P2P-Streaming-Software* manifestiert sich der Wille der Anbieter zur Herstellung urheberrechtswidriger Werkvervielfältigungen i.S.v. Art. 67 Abs. 1 lit. e URG. Da die *P2P-Streaming-Software* praktisch ausschliesslich zu illegalen Zwecken eingesetzt wird, müssen die Anbieter zumindest in Kauf nehmen, dass diese zur Begehung von Urheberrechtsverletzungen verwendet wird.<sup>825</sup>

*cc) Rechtswidrigkeit und Schuld*

Es sind vorliegend kaum Rechtfertigungs- oder Schuldausschlussgründe denkbar. Auch ein beachtlicher Rechtsirrtum scheint ausgeschlossen.

*d) Anstiftung*

Mangels Einwirkung auf die Willensbildung des Täters ein Verbrechen oder Vergehen zu verüben, scheidet eine Bestrafung wegen Anstiftung nach Art. 24 StGB aus.<sup>826</sup>

*e) Gehilfenschaft*

Falls eine mittäterschaftliche Tatbegehung in der vorliegenden Konstellation abgelehnt wird, ist sodann eine Gehilfenschaft zu einer Urheberrechtsverletzung nach Art. 67 Abs. 1 lit. e URG zu prüfen. Gehilfe i.S.v. Art. 25 StGB ist, wer zu einem Verbrechen oder Vergehen vorsätzlich Hilfe leistet.<sup>827</sup>

*aa) Objektiver Tatbestand*

Der relevante Förderungsbeitrag der Anbieter liegt im Bereithalten der *P2P-Streaming-Software* sowie im Unterhalt derselben. Der Unterhalt der Web-

---

<sup>824</sup> BGE 125 IV 134, Erw. 3a.

<sup>825</sup> S.o. Rz. 343.

<sup>826</sup> S.o. Rz. 346.

<sup>827</sup> Urteil 6B\_757/2010 des Bundesgerichts vom 7. Februar 2011, Erw. 4.1.

seite, das Aktualisieren der Software sowie das Anbieten von *Links* auf die urheberrechtswidrig angebotenen geschützten Inhalte ist als aktive Hilfeleistung zur unerlaubten Herstellung von Werkexemplaren zu qualifizieren.<sup>828</sup> Die Beihilfehandlung könnte auch in einer Unterlassung der Einstellung des Anbietens der Software gesehen werden.<sup>829</sup> Da bei der Herstellung der Werkkopien auf dem Nutzerrechner im Rahmen des *P2P-Streaming* in den meisten Fällen keine Einwilligung der Rechteinhaber vorliegt, ist das objektive Tatbestandsmerkmal der Unrechtmässigkeit zu bejahen.<sup>830</sup>

*bb) Subjektiver Tatbestand*

- 362 Der (Eventual-)Vorsatz des Gehilfen muss sich „sowohl auf die Haupttat wie auch auf die eigene Beihilfehandlung beziehen“<sup>831</sup>. Die Anbieter der *P2P-Streaming-Software* wissen Bescheid um deren technische Funktionsweise sowie den Umstand, dass die im Rahmen des *P2P-Streamings* hergestellten Werkkopien als unerlaubte Herstellung eines Werkexemplars zu qualifizieren sind (Art. 67 Abs. 1 lit. e i.V.m. Art. 10 Abs. 2 lit. a URG).<sup>832</sup>
- 363 Wie bereits zuvor aufgezeigt ist in dieser Konstellation lediglich fraglich, ob im Zeitpunkt der Hilfeleistung, d.h. des Anbietens der *P2P-Streaming-Software*, der Tatentschluss des Täters bereits gefasst worden sein muss.<sup>833</sup> Für die Anbieter der *P2P-Streaming-Software* war es unstrittig vorhersehbar, dass die Software zur Begehung von Urheberrechtsverletzungen genutzt werden würde – wurde sie doch genau zu diesem Zweck programmiert.

*cc) Rechtswidrigkeit und Schuld*

- 364 Es sind kaum Rechtfertigungs- oder Schuldausschlussgründe ersichtlich, auf welche sich die Anbieter der *P2P-Streaming-Software* berufen können. Insbesondere fällt ein beachtlicher Rechtsirrtum ausser Betracht, da die Anbieter die Strafbarkeit ihres Handelns hätten erkennen können, wenn sie – unter Anwendung der gebotenen Sorgfalt – vorgängige Abklärungen getroffen hätten.

---

<sup>828</sup> S.o. Rz. 349; Urteil 6B\_757/2010 des Bundesgerichts vom 7. Februar 2011, Erw. 4.4.; SCHWARZENEGGER, P2P-Netzwerke, 232.

<sup>829</sup> S.o. Rz. 350; SCHWARZENEGGER, P2P-Netzwerke, 243 f.

<sup>830</sup> SCHWARZENEGGER, P2P-Netzwerke, 218, GLARNER, Musikpiraterie im Internet, 73 ff.

<sup>831</sup> BGE 121 IV 109, Erw. 3a; FORSTER, BSK StGB I, Art. 25 N 3.

<sup>832</sup> S.o. Rz. 330 ff.

<sup>833</sup> S.o. Rz. 352; SCHWARZENEGGER, P2P-Netzwerke, 242 f.

## 2. Strafbarkeit involvierter Anonymisierungsdienste

Auf der Webseite von *Time4Popcorn.eu* wurde die *P2P-Streaming-Software* 365 u.a. damit beworben, dass diese über einen integrierten *VPN-Client* verfügt.<sup>834</sup> Der Anonymisierungsdienst soll die Aufzeichnung von Übermittlungsdaten verhindern und insbesondere die IP-Adressen der am *P2P-Netzwerk* beteiligten Nutzer verschleiern, um dadurch eine Identifikation der jeweiligen Anschlussinhaber zu erschweren bzw. zu verunmöglichen.<sup>835</sup> Da die Betreiber der Anonymisierungssoftware selbst keine rechtswidrigen Handlungen an urheberrechtlich geschützten Werken vornehmen, ist eine Strafbarkeit wegen Alleintäterschaft ausgeschlossen. Mit Blick auf die Anonymisierungsdienste ist daher die Mittäterschaft oder die Gehilfenschaft zu einer Urheberrechtsverletzung nach Art. 67 URG zu prüfen.

### A. Mittäterschaft

Massgebend für die mittäterschaftliche Beteiligung ist die Rolle, welche der Einzelne willentlich übernimmt.<sup>836</sup> Der Tatbeitrag des Anonymisierungsdienstes beschränkt sich vorliegend auf die Verschlüsselung des Datenverkehrs innerhalb des *P2P-Netzwerks*. Da die Anonymisierungsdienste hinsichtlich der unerlaubten Zugänglichmachung von Werken bzw. der unerlaubten Herstellung von Werkexemplaren über keine Tatherrschaft verfügen, fällt die mittäterschaftliche Begehung einer Urheberrechtsverletzung nach Art. 67 URG ausser Betracht.

### B. Gehilfenschaft

#### a) Objektiver Tatbestand

Die Gehilfenschaft zu einer unerlaubten Zugänglichmachung (Art. 67 Abs. 1 367 lit. g<sup>bis</sup> URG i.V.m. Art. 25 StGB) bzw. einer unerlaubten Herstellung von Werkexemplaren (Art. 67 Abs. 1 lit. e URG i.V.m. Art. 25 StGB) setzt in

---

<sup>834</sup> Angeblich stand der VPN-Dienst Kebrum dahinter, der für Werbezwecke seinen Verschlüsselungsdienst kostenlos zur Verfügung gestellt hatte; VAN DER SAR, <<https://torrentfreak.com/popcorn-time-gives-users-anonymity-with-a-free-built-in-vpn-140607/>> (besucht 25. August 2015); vgl. auch <<http://time4popcorn.se>> (besucht 25. August 2015), wo ebenfalls mit einem eingebauten *VPN-Client* geworben wird.

<sup>835</sup> Vgl. auch GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 24, die auf die Problematik des anonymisierten Datenaustausches in *P2P-Netzwerken* hinweisen.

<sup>836</sup> Urteil 6B\_939/2013 des Bundesgerichts vom 17. Juni 2014, Erw. 2.

objektiver Hinsicht eine rechtswidrige, tatbestandsmässige Haupttat eines anderen sowie eine diese Haupttat fördernde Handlung des Gehilfen voraus. Weil der Datenaustausch zwischen den beteiligten Nutzern durch die Verschlüsselung des Anonymisierungsdienstes nicht gefördert wird, fällt eine physische Gehilfenschaft vorliegend ausser Betracht. Denkbar wäre jedoch eine psychische Gehilfenschaft. Eine solche liegt vor, wenn der Gehilfe den Täter durch sein Verhalten in der Ausführung seiner Tat bestärkt, seinen Tatentschluss stützt oder fördert.<sup>837</sup>

- 368 Die Anbieter der *P2P-Streaming-Software* bewerben ihren Dienst mitunter damit, dass der Datenaustausch zwischen den Nutzern anonym stattfindet. Die Zusicherung der Anonymität innerhalb des *P2P-Streaming-Netzwerks* kann sich motivierend auf die Nutzer auswirken, am illegalen *P2P-Streaming* zu partizipieren, da diesen suggeriert wird, dass sie dabei keine urheberstrafrechtlichen Konsequenzen zu befürchten hätten.<sup>838</sup> Indem ein Anonymisierungsdienst den Datenverkehr eines illegalen *P2P-Streaming-Dienstes* verschlüsselt, fördert er die Bereitschaft der Nutzer zur Begehung von Urheberrechtsverletzungen nach Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG.<sup>839</sup>

#### **b) Subjektiver Tatbestand**

- 369 Der (Eventual-)Vorsatz des Gehilfen muss sich auf die Haupttat sowie auf die eigene Hilfeleistung beziehen.<sup>840</sup> Die Betreiber des Anonymisierungsdienstes handeln in Kenntnis über die Urheberrechtswidrigkeit des *P2P-Streaming-Dienstes*. Sie wissen um die psychische Gehilfenschaft ihrer Hilfeleistung Bescheid und handeln mit der Absicht, die Nutzer zur Begehung von Urheberrechtsverletzungen nach Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG zu motivieren, um dadurch die Popularität des eigenen Anonymisierungsdienstes zu steigern.

---

<sup>837</sup> DONATSCH/TAG, 169; Urteil 6S.167/2004 des Bundesgerichts vom 8. Juli 2004, Erw. 2.3.

<sup>838</sup> Vgl. SCHEDER-BIESCHIN, 139, wonach bei gefahrgeneigten Diensten die Schaffung einer „Umgebung der aktiven Anonymität“ massenhaften Urheberrechtsverletzungen Vorschub leistet.

<sup>839</sup> Zur Strafrechtlichen Verantwortlichkeit des Unternehmens siehe Art. 102 StGB; FORSTER, 203 ff.

<sup>840</sup> DONATSCH/TAG, 170.

**c)      *Rechtswidrigkeit und Schuld***

Es sind weder Rechtfertigungs- noch Schuldausschlussgründe ersichtlich. 370  
Auch ein beachtlicher Rechtsirrtum nach Art. 21 StGB fällt ausser Betracht.

**3.      Strafbarkeit der *Hosting-Provider***

**A.      Alleintäterschaft**

Im Unterschied zum *Server-Streaming*<sup>841</sup> werden beim *P2P-Streaming* die 371  
Inhalte nicht auf zentralen *Servern* gespeichert und an die Nutzer verteilt,  
sondern zwischen den Nutzern direkt ausgetauscht.<sup>842</sup> Der Tatbeitrag des  
*Hosting-Providers* beschränkt sich auf das *Hosting* der Webseite, über wel-  
che die *P2P-Streaming-Software* durch die Nutzer abgerufen bzw. herunter-  
geladen werden kann.<sup>843</sup> Eine unerlaubte Zugänglichmachung von Werken  
nach Art. 67 Abs. 1 lit. g<sup>bis</sup> URG ist deshalb zu verneinen, da die geschützten  
Werke nicht durch die *Hosting-Provider* zugänglich gemacht werden.

**B.      Mittäterschaft**

Auch eine Mittäterschaft ist mit Blick auf die *Hosting-Provider* abzulehnen, 372  
da sich deren Tatbeitrag im *Hosting* von Webseiten erschöpft. Im Normalfall  
haben die *Hosting-Provider* keine Kenntnis von den auf diesen Webseiten  
veröffentlichten Inhalten und können diese auch nicht kontrollieren. Die  
*Hosting-Provider* wirken weder in „massgebender Weise“ bei der Tatausfüh-  
rung mit, noch ist deren Tatbeitrag derart wichtig, dass diese als Hauptbetei-  
ligte erscheinen.<sup>844</sup> Eine Mittäterschaft der *Hosting-Provider* ist deshalb  
abzulehnen.

**C.      Gehilfenschaft**

Unternimmt der *Hosting-Provider* trotz Hinweisen nichts, um die Verbrei- 373  
tung der *P2P-Streaming-Software* über dessen *Server* zu verhindern, ist eine  
Gehilfenschaft zur unerlaubten Zugänglichmachung von Werken durch Un-

---

<sup>841</sup> KUROSE/ROSS, 647; VON GERLACH, 53.

<sup>842</sup> VON GERLACH, 67.

<sup>843</sup> Die Software muss sich nicht zwingend auf demselben *Server* befinden.

<sup>844</sup> FORSTER, BSK StGB I, N 9 Vorb. zu Art. 24; BGE 133 IV 76, Erw. 2.7; 130 IV 58,  
Erw. 9.2.1; 125 IV 134, Erw. 3a.

terlassung i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG i.V.m. Art. 25 i.V.m. Art. 11 StGB zu prüfen.<sup>845</sup> Der fördernde Tatbeitrag des *Hosting-Providers* besteht darin, dass dieser es unterlässt, die Webseite, über welche die *P2P-Streaming-Software* angeboten wird, von seinen *Servern* zu entfernen. An dieser Stelle muss daher geprüft werden, ob die *Hosting-Provider* überhaupt eine Pflicht trifft, die Software nach erlangter Kenntnis von deren *Servern* zu entfernen (Garantenstellung).

- 374 Eine solche Pflicht liesse sich allenfalls aus Ziff. 7.1 des *Code of Conduct Hosting (CCH)* herleiten, wonach der *Hosting-Provider* den Zugang zu einer Webseite nach eigenem Ermessen ganz oder teilweise sperren kann, wenn diese mit hoher Wahrscheinlichkeit unzulässige Inhalte enthält.<sup>846</sup> Da der *CCH* auf der Basis freiwilliger Abmachungen beruht und die Sperrung einschlägiger Webseiten im Ermessen der *Hosting-Provider* liegt, kann eine Pflicht der *Hosting-Provider* zur Entfernung urheberrechtsverletzender Inhalte, nicht pauschal als gegeben angenommen werden. Eine Gehilfenschaft der *Hosting-Provider* zur unerlaubten Zugänglichmachung von Werken durch Unterlassen i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG i.V.m. Art. 11 Abs. 2 und 3 StGB ist deshalb abzulehnen.<sup>847</sup>

### III. Legale Nutzungsmöglichkeiten von *P2P-Streaming*

- 375 Neben illegalen *P2P-Plattformen* sind auch legale Einsatzmöglichkeiten der *P2P-Streaming-Technologie* zur Verbreitung urheberrechtlich geschützter Werke denkbar.<sup>848</sup> So hat sich beispielsweise der Streaming-Dienst *Netflix*

---

<sup>845</sup> SCHWARZENEGGER, P2P-Netzwerke, 247, m.w.H.

<sup>846</sup> <<http://tinyurl.com/SIMSA-Code-of-Conduct-Hosting>> (besucht 25. August 2015); DE WERRA, sic! 2014, 199 f.

<sup>847</sup> Problematisch ist auch, dass die *Hosting-Provider* andernfalls für eine Überprüfung und Sperrung der von ihnen gehosteten Webseiten verantwortlich wären. Hinzu kommt, dass die *Hosting-Provider* technisch nicht in der Lage sind, einzelne (urheberrechtswidrige) Inhalte auf einer Webseite entfernen können, sondern lediglich den Zugang zu einer Webseite ganz oder teilweise blockieren können.

<sup>848</sup> KUROSE/ROSS, 647, verweisen auf das chinesische Unternehmen Xunlei Kankan, welches eine hybride *CDN-P2P*-Architektur für das Video-on-Demand-Streaming verwendet; ausführlich dazu ZHANG/LIU/HEI/CHENG, IEEE Transactions on Multimedia 2015, 229 ff.

damit beschäftigt, wie diese Technologie für das legale, kommerzielle Streaming urheberrechtlich geschützter Inhalte eingesetzt werden könnte.<sup>849</sup>

Die Idee des Einsatzes der *P2P-Technologie* zur Distribution geschützter 376 Werke erscheint zukunftsweisend. Die Audio-/Video-Dateien werden in zunehmend höherer Auflösung produziert und die Zahl der Nutzer von Streaming-Plattformen nimmt ebenfalls zu. Die *P2P-Technologie* würde die technischen und finanziellen Ressourcen der Anbieter entlasten, da nicht mehr sämtliche Inhalte von eigenen *Servern* an die Nutzer übertragen werden müssen.<sup>850</sup> Aus rechtlicher Perspektive setzt dies eine Einwilligung der Rechteinhaber voraus, dass sämtliche der am *P2P-Netzwerk* beteiligten Personen die geschützten Inhalte temporär vervielfältigen und mittels *Upload* untereinander weiterverbreiten dürfen.<sup>851</sup> Sodann muss technisch durch die Verwendung geeigneter Software sichergestellt werden, dass die Weiterverbreitung nur innerhalb eines bestimmten Nutzerkreises möglich bleibt, welcher die Nutzungsbedingungen der Rechteinhaber respektiert.

---

<sup>849</sup> BRODKIN, <<http://arstechnica.com/information-technology/2014/04/netflix-researching-large-scale-peer-to-peer-technology-for-streaming>> oder VAN DER SAR <<https://torrentfreak.com/netflix-needs-bittorrent-expert-to-implement-p2p-streaming-150520>> (beide besucht 25. August 2015).

<sup>850</sup> ZHANG/LIU/HEI/CHENG, IEEE Transactions on Multimedia 2015, 229; KUROSE/ROSS, 647.

<sup>851</sup> Art. 10 Abs. 2 lit. a und lit. c URG.

## 5. Teil: Rechtsdurchsetzung bei Urheberrechtsverletzungen im Rahmen des Streaming

- <sup>377</sup> Die Rechtsdurchsetzung bei Urheberrechtsverletzungen im Internet gestaltet sich in vielerlei Hinsicht als eine komplizierte Angelegenheit.<sup>852</sup> Eine funktionierende Internetverbindung vorausgesetzt, können aufgrund der Globalität des Internets urheberrechtlich geschützte Inhalte von jedermann weltweit hochgeladen, weiterverbreitet und abgerufen werden. Die Betreiber illegaler Plattformen machen sich diesen Umstand zunutze, indem sie von Staaten aus operieren, in denen Urheberrechtsverletzungen bekanntermassen nicht (wirksam) verfolgt und bestraft werden.<sup>853</sup> Hinzu kommt die Problematik, dass eine effektive Strafverfolgung im Internet durch die Anonymität der Nutzer zusätzlich erschwert wird.<sup>854</sup>
- <sup>378</sup> Das Eidgenössische Justiz- und Polizeidepartement (EJPD) hat am 8. August 2012 eine Arbeitsgruppe zur Optimierung der kollektiven Verwertung von Urheberrechten und verwandten Schutzrechten (AGUR12<sup>855</sup>) einberufen und damit beauftragt, bis Ende 2013 in einem Bericht die Möglichkeiten zur Anpassung des Urheberrechts an die technischen Entwicklungen aufzuzeigen.<sup>856</sup> Am 6. Dezember 2013 veröffentlichte die AGUR12 ihren Schlussbericht. Darin wird ein Massnahmenpaket mit fünf Schwerpunkten vorgeschlagen: eine Verbesserung der Information der Konsumenten, legale Angebote sollen ausgebaut und deren Attraktivität gesteigert werden, die Bekämpfung von Urheberrechtsverletzungen soll vereinfacht werden und zudem soll eine Steigerung der Effizienz und der Transparenz der Verwertungsgesellschaften sowie eine Anpassung der urheberrechtlichen Schrankenregelungen an die neuesten Entwicklungen stattfinden.<sup>857</sup> Gemäss einer Medienmitteilung vom 6. Juni 2014 plant der Bundesrat eine Modernisierung des Urheberrechts, um dieses an die Gegebenheiten des Internetzeitalters anzupassen. Gestützt auf

---

<sup>852</sup> BECHTOLD, ZSR 2015 II, 103; WULLSCHLEGER, Rz. 1 ff.; THOUVENIN, sic! 2009, 100; BAUMGARTNER, 205 ff.; GLARNER, Musikpiraterie im Internet, 146.

<sup>853</sup> SPINDLER, NJW 2014, 2553; GLARNER, Musikpiraterie im Internet, 146.

<sup>854</sup> SCHEDER-BIESCHIN, 5; THOUVENIN, sic! 2009, 100.

<sup>855</sup> Die Arbeitsgruppe setzte sich zusammen aus Kunschtschaffenden sowie Vertreterinnen und Vertretern der Produzenten, der Wirtschaft, der Nutzer und der Konsumenten.

<sup>856</sup> <<https://www.ige.ch/urheberrecht/agur12.html>> (besucht 25. August 2015).

<sup>857</sup> EGLI, Jusletter vom 25. August 2014, Rz. 33.



Empfehlungen, welche die AGUR12 verabschiedet hat, soll das Eidgenössische Justiz- und Polizeidepartement (EJPD) bis Ende 2015 eine Vorlage für die Vernehmlassung erarbeiten.<sup>858</sup>

## **I. Datenbearbeitung zur Ermittlung von Urheberrechtsverletzern im Internet**

### **1. Probleme bei der Ermittlung der Täterschaft bei Urheberrechtsverletzungen im Internet *de lege lata***

#### **A. Anonymität im Internet**

Die Verfolgung von über das Internet begangenen Straftaten wird durch den 379 Umstand erschwert, dass die Nutzer dabei mehr oder weniger anonym agieren. Selbst nach erfolgter Feststellung durch die Rechteinhaber, dass ihre Werke etwa über *P2P-Netzwerke* zwischen den beteiligten Nutzern unerlaubt ausgetauscht werden, können diese nicht direkt gegen die Urheberrechtsverletzer vorgehen, da deren Identität vorerst unbekannt ist. Der (häufig) einzige Anknüpfungspunkt ist die IP-Adresse der Anschlussinhaber der am *P2P-Netzwerk* beteiligten Nutzer.<sup>859</sup> Ausgehend vom „*Logistep-Entscheid*“<sup>860</sup> sollen – anhand einer Analyse von Lehre und Rechtsprechung – die datenschutzrechtlichen Schwierigkeiten der softwareunterstützten Aufzeichnung von Nutzerdaten (insbesondere der IP-Adressen) zur Identitätsermittlung bei Urheberrechtsverletzungen in *P2P-Netzwerken* aufgezeigt werden.

---

<sup>858</sup> <<http://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2014/2014-06-061.html>> (besucht 25. August 2015).

<sup>859</sup> WULLSCHLEGER, Rz. 19 ff., mit ausführlichen technischen Hinweisen zur Identifizierung des Urheberrechtsverletzers über dessen *IP-Adresse*; GLESS, ZStrR 2012, 13; THOUVENIN, ACTA, 106; HENNEMANN, 246; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 24; BISGES, wistra 2009, 303 ff.; THOUVENIN, sic! 2009, 100; Der Inhaber des Internetanschlusses muss nicht identisch mit der die Urheberrechtsverletzung begehenden Person sein. Zudem kann die *IP-Adresse* auch verschleiert werden, falls die Nutzer einen Anonymisierungsdienst (*TOR*, *JonDo*) verwenden. Die Rechtslage gestaltet sich beim *P2P-Streaming* gleich wie bei herkömmlichen *P2P-Netzwerken* mit *Download*-Funktion, da in beiden Fällen eine unerlaubte Herstellung von Werkexemplaren sowie eine unerlaubte Zugänglichmachung von Werken gem. Art. 67 Abs. 1 lit. e bzw. lit. g<sup>bis</sup> URG vorliegt.

<sup>860</sup> BGE 136 II 508.

a) **Der „Logistep-Entscheid“**

- 380 Die Firma Logistep AG hatte – im Auftrag der Rechteinhaber – mit einer eigens von ihr entwickelten Software diverse *P2P-Netzwerke* nach widerrechtlich angebotenen, geschützten Werken durchsucht.<sup>861</sup> Beim Herunterladen der Werke wurden die Benutzernamen, die IP-Adressen der verwendeten Internetanschlüsse, die Identifikationsnummern der vom Anbieter des urheberrechtlich geschützten Werks verwendeten Software (GUID), die verwendeten *P2P-Netzwerkprotokolle*, der Name und der elektronische Fingerabdruck (Hashcode) des geschützten Werks sowie das Datum, die Uhrzeit und der Zeitraum der Verbindung zwischen der Software der Logistep AG und der Software der Anbieter des urheberrechtlich geschützten Werks aufgezeichnet und in einer Datenbank abgespeichert.<sup>862</sup>

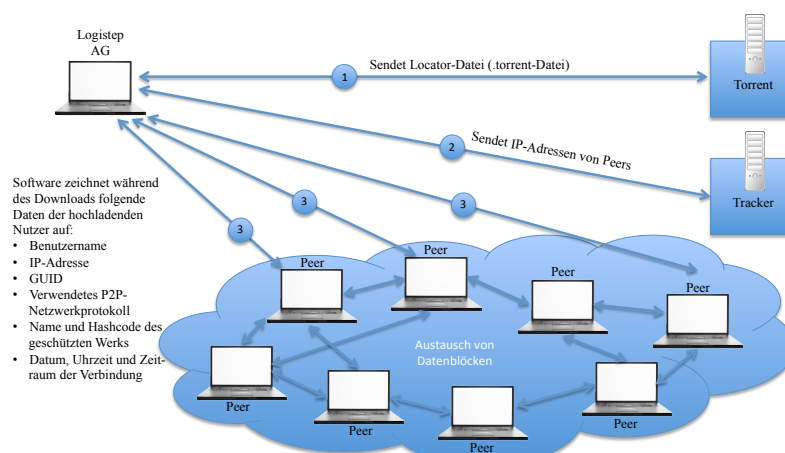


Abbildung 14: Datenverteilung mit BitTorrent, Quelle: TANENBAUM/WETHERALL, 850.

- 381 Mit den von Logistep gesammelten Daten leiteten die Rechteinhaber ein Strafverfahren gegen Unbekannt ein.<sup>863</sup> Im Falle einer über das Internet begangenen Straftat sind die *Access-Provider* gestützt auf Art. 14 Abs. 4 BÜPF verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine

<sup>861</sup> PROBST, AJP 2013, 1429; SCHÄFER/DORDI, medialex 2011, 142; RUDIN, digma 2011, 144 f.; SCHWEIZER/BISCHOF, digma 2011, 152 ff.; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 1; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 1.

<sup>862</sup> SCHÄFER/DORDI, medialex 2011, 143; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 1; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 1.

<sup>863</sup> SCHÄFER/DORDI, medialex 2011, 143; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 1.

Identifikation der Anschlussinhaber ermöglichen.<sup>864</sup> Gestützt auf das Akteneinsichtsrecht konnten sich die Rechteinhaber als Geschädigte im Strafverfahren Kenntnis von der Identität der Personen verschaffen, über deren Internetanschluss die Werke in urheberrechtsverletzender Weise angeboten und verbreitet worden sind.<sup>865</sup> Anhand der Personendaten konnten die Rechteinhaber nun auch zivilrechtlich gegen diese Personen vorgehen.<sup>866</sup> Die zivilrechtlichen Verfahren wurden i.d.R. durch eine Abmahnung mit Zahlungsaufforderung eingeleitet und endeten regelmässig mit einem Vergleich.<sup>867</sup>

*aa) Empfehlung des EDÖB*

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) 382 qualifizierte die Bearbeitungsmethoden der Logistep AG als datenschutzwidrig und empfahl dieser, gestützt auf Art. 29 Abs. 3 DSG, die Datenbearbeitung unverzüglich einzustellen, solange keine ausreichende gesetzliche Grundlage für die zivilrechtliche Nutzung der so erhobenen Daten besteht.<sup>868</sup> Nach Ansicht des EDÖB lag in der von der Logistep AG vorgenommenen Datenbearbeitung eine Verletzung von Art. 12 Abs. 2 lit. a DSG vor.<sup>869</sup> Konkret sah der EDÖB in der von der Firma Logistep AG vorgenommenen Datenbearbeitung Verstösse gegen das Zweckmässigkeitsprinzip (Art. 4 Abs. 3 DSG) sowie das Erkennbarkeitsprinzip (Art. 4 Abs. 4 DSG).<sup>870</sup> Weiter hielt der EDÖB fest, dass im Rahmen einer rein zivilrechtlichen Geltendmachung von Schadenersatzansprüchen im vorliegenden Fall ein überwiegendes privates Interesse der Urheberrechtsinhaber abgelehnt werden müsse.<sup>871</sup> Darüber hinaus qualifizierte der EDÖB das Vorgehen der Logistep AG als Verstoß gegen den Grundsatz von Treu und Glauben, weshalb sich eine

---

<sup>864</sup> GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 3; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 1.

<sup>865</sup> SCHÄFER/DORDI, medialex 2011, 143; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 3, sprechen daher „von der Identität der vermeintlichen Raubkopierer“; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 1.

<sup>866</sup> GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 3; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 1.

<sup>867</sup> PROBST, AJP 2013, 1429; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 3; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 1.

<sup>868</sup> Empfehlung EDÖB, Ziff. 1; SCHÄFER/DORDI, medialex 2011, 142; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 4; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 2.

<sup>869</sup> Empfehlung EDÖB, Erw. 5; SCHÄFER/DORDI, medialex 2011, 143.

<sup>870</sup> Empfehlung EDÖB, Erw. 5; SCHÄFER/DORDI, medialex 2011, 143.

<sup>871</sup> Empfehlung EDÖB, Erw. 13.

Verhältnismässigkeitsprüfung für die Datenerhebung im Hinblick auf die Anstrengung eines Zivilverfahrens erübrigen würde.<sup>872</sup> Falls eine Durchbrechung des Fernmeldegeheimnisses im Rahmen eines Zivilverfahrens ermöglicht werden soll, bedarf es hierzu – nach Meinung des EDÖB – einer gesetzlichen Grundlage, die analog zum BÜPF im Strafverfahren die Bedingungen für eine Durchbrechung des Fernmeldegeheimnisses regelt.<sup>873</sup> Das Vorliegen von Rechtfertigungsgründen nach Art. 13 Abs. 1 DSG für die verursachte Persönlichkeitsverletzung wurde vom EDÖB verneint.<sup>874</sup>

*bb) Entscheid des Bundesverwaltungsgerichts*

- 383 Nachdem die Logistep AG die Empfehlung des EDÖB abgelehnt hatte, legte der EDÖB die Angelegenheit mit Klage vom 13. Juni 2008 dem Bundesverwaltungsgericht zur Entscheidung vor.<sup>875</sup> In seinem Verdikt bejahte das Bundesverwaltungsgericht, dass IP-Adressen als Personendaten i.S.d. DSG anzusehen sind.<sup>876</sup> Weiter taxierte das Bundesverwaltungsgericht, dass die Bestimmung von Art. 2 Abs. 2 lit. c DSG, wonach das DSG nicht auf hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren anwendbar ist, in der vorliegenden Sachverhaltskonstellation als nicht einschlägig, da zum Zeitpunkt der Datenbearbeitung noch nicht bekannt sei, gegen wen sich ein allfälliges Verfahren richtet.<sup>877</sup> Da die Logistep AG ihren Sitz in Steinhausen im Kanton Zug hatte, sah das Bundesverwaltungsgericht auch den räumlichen Geltungsbereich des DSG als gegeben an.<sup>878</sup> Schliesslich bejahte das Bundesverwaltungsgericht auch das Vorliegen eines Systemfehlers i.S.v. Art. 29 Abs. 1 lit. a DSG, da das Sammeln von Personendaten (*IP-Adressen*) von Teilnehmern in *P2P*-

---

<sup>872</sup> Empfehlung EDÖB, Erw. 13.

<sup>873</sup> Empfehlung EDÖB, Erw. 13; SCHÄFER/DORDI, *medialex* 2011, 143.

<sup>874</sup> Empfehlung EDÖB, Erw. 13 ff.; SCHÄFER/DORDI, *medialex* 2011, 143.

<sup>875</sup> SCHÄFER/DORDI, *medialex* 2011, 143.

<sup>876</sup> Urteil A-3144/2008 des Bundesverwaltungsgerichts vom 27. Mai 2009, Erw. 2.2, mit dem Hinweis, dass es sich bei *IP-Adressen* nicht um besonders schützenswerte Personendaten gem. Art. 3 lit. c Ziff. 4 DSG handeln würde; SCHÄFER/DORDI, *medialex* 2011, 143; SCHWARZENEGGER, *P2P-Netzwerke*, 248 f.

<sup>877</sup> Urteil A-3144/2008 des Bundesverwaltungsgerichts vom 27. Mai 2009, Erw. 3; DROESE, 262 ff.

<sup>878</sup> Urteil A-3144/2008 des Bundesverwaltungsgerichts vom 27. Mai 2009, Erw. 4.

*Netzwerken* geeignet sei, um eine grössere Anzahl von Personen in deren Persönlichkeit zu verletzen und trat auf die Klage des EDÖB ein.<sup>879</sup>

In materieller Hinsicht prüfte das Bundesverwaltungsgericht die Rechtmässigkeit der Bearbeitung der Personendaten durch die Logistep AG und stellte fest, dass das in Art. 4 Abs. 1 DSG verankerte Rechtmässigkeitsprinzip durch das Vorgehen der Logistep AG nicht verletzt wurde. Weiter beurteilte das Bundesverwaltungsgericht das Vorgehen der Logistep AG als „Reaktion auf vorangegangene oder zumindest vermutete Rechtsverletzungen“ als mit dem Grundsatz von Treu und Glauben vereinbar.<sup>880</sup>

Schliesslich hielt das Bundesverwaltungsgericht fest, dass die Verletzung der Persönlichkeitsrechte der am *P2P-Netzwerk* beteiligten Nutzer vorliegend durch überwiegende private und öffentliche Interessen (Art. 13 Abs. 1 DSG) gerechtfertigt und damit nicht widerrechtlich sei.<sup>881</sup> Konkret würde das öffentliche Interesse an der Durchsetzung bestehenden Rechts sowie die Interessen der Urheberrechtsinhaber respektive der Logistep AG die Interessen der von der Datenbearbeitung betroffenen Personen, überwiegen.<sup>882</sup>

cc) *Entscheid des Bundesgerichts*

Gegen dieses Urteil erhob der EDÖB am 26. Juni 2009 Beschwerde in öffentlich-rechtlichen Angelegenheiten, auf die das Bundesgericht eintrat.<sup>883</sup> Wie schon das Bundesverwaltungsgericht qualifizierte auch das Bundesgericht die bearbeiteten *IP-Adressen* als Personendaten i.S.v. Art. 3 lit. a DSG.<sup>884</sup> Übereinstimmend mit der Vorinstanz stellte das Bundesgericht fest, dass die Logistep AG gegen die in Art. 4 Abs. 3 und Abs. 4 DSG statuierten

---

<sup>879</sup> Urteil A-3144/2008 des Bundesverwaltungsgerichts vom 27. Mai 2009, Erw. 5.1.1; SCHÄFER/DORDI, *medialex* 2011, 143.

<sup>880</sup> Urteil A-3144/2008 des Bundesverwaltungsgerichts vom 27. Mai 2009, Erw. 9.3, wonach auch der Umstand, dass die Datenbearbeitung durch die Logistep AG regelmässig mit einer Verletzung des Erkennbarkeitsprinzips einhergehe, nichts an dieser Feststellung zu ändern vermag.

<sup>881</sup> Urteil A-3144/2008 des Bundesverwaltungsgerichts vom 27. Mai 2009, Erw. 12.3.2.

<sup>882</sup> Urteil A-3144/2008 des Bundesverwaltungsgerichts vom 27. Mai 2009, Erw. 12.3.2.

<sup>883</sup> <<http://www.edoeb.admin.ch/datenschutz/00628/00664/index.html?lang=de>> (besucht 25. August 2015); SCHÄFER/DORDI, *medialex* 2011, 144.

<sup>884</sup> BGE 136 II 508, Erw. 3.8; WULLSCHLEGER, Rz. 48 ff., m.w.H.; a.A. PROBST, AJP 2013, 1430, der an dieser Betrachtungsweise kritisiert, dass sie „in einer globalisierten Informationsgesellschaft auf eine Beseitigung der gesetzlichen Unterscheidung zwischen Personendaten und anonymen Einzeldaten (als Nicht-Personendaten) hinausläuft [...]“.

Grundsätze der Zweckbindung und der Erkennbarkeit verstossen habe, da sie ohne das Wissen der Betroffenen Daten gesammelt hat und bejahte eine Persönlichkeitsverletzung nach Art. 12 Abs. 2 lit. a DSG.<sup>885</sup> Obschon die aktuelle Fassung von Art. 12 Abs. 2 lit. a DSG – im Unterschied zu Art. 12 Abs. 2 lit. b und c DSG – keinen expliziten Hinweis auf die Rechtfertigungsgründe enthält, stellte das Bundesgericht klar, dass diese auch bei Verletzung der Datenbearbeitungsgrundsätze Anwendung finden.<sup>886</sup> Die Bestimmung sei so auszulegen, dass „eine Rechtfertigung der Bearbeitung von Personendaten entgegen der Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 DSG zwar nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall aber nur mit grosser Zurückhaltung bejaht werden können“<sup>887</sup>. Insbesondere sei zu berücksichtigen, dass der EDÖB in einem Rahmen handelt, der über das reine Zweiparteienverhältnis hinausgeht.<sup>888</sup> Die Bedeutung der Empfehlung des EDÖB sei deshalb bei der Abwägung der Interessen nach Art. 13 Abs. 1 DSG zu berücksichtigen.<sup>889</sup>

- 387 SCHÄFER/DORDI führen dazu aus, dass das Bundesverwaltungsgericht eine eher individualistisch geprägte Sichtweise eingenommen und den durch die Datenbearbeitung der Logistep AG verursachten Eingriff in die Persönlichkeitsrechte der betroffenen Personen den in ihren Rechten verletzten Rechteinhabern gegenübergestellt habe, während das Bundesgericht zudem die „gesamtgesellschaftliche Wirkung“ der Eingriffe in die Persönlichkeitsrechte der Betroffenen als weitere Komponente in seine Erwägungen eingeschlossen habe.<sup>890</sup> Das Bundesgericht war der Ansicht, dass die von der Logistep AG gewählte Bearbeitungsmethode „allgemein – über den konkreten Fall hinaus – wegen fehlender gesetzlicher Reglementierung in diesem Bereich zu einer Unsicherheit in Bezug auf die im Internet angewendeten Methoden

---

<sup>885</sup> BGE 136 II 508, Erw. 6.3.4; SCHÄFER/DORDI, *medialex* 2011, 144; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 11 und ROSENTHAL, Jusletter vom 27. September 2010, Rz. 4.

<sup>886</sup> BGE 136 II 508, Erw. 5.2.4.; SCHÄFER/DORDI, *medialex* 2011, 144 m.w.H.

<sup>887</sup> BGE 136 II 508, Erw. 5.2.4.

<sup>888</sup> BGE 136 II 508, Erw. 6.3.2; SCHÄFER/DORDI, *medialex* 2011, 145 ff.

<sup>889</sup> BGE 136 II 508, Erw. 6.3.2; SCHÄFER/DORDI, *medialex* 2011, 146 f., sind der Meinung, dass die durch die Logistep AG verursachte Persönlichkeitsverletzung zu einer Unsicherheit in der Gesellschaft punkto Datenbearbeitung führen könne, die geeignet sei, das Vertrauen der Gesellschaft zu erschüttern; a.A. ROSENTHAL, *digma* 2011, 41, der zu bedenken gibt, dass das für eine Interessenabwägung relevante Datenschutzinteresse einer einzelnen Person gegen die Bearbeitung ihrer Daten nicht deshalb schwerer wiegt, weil noch andere Personen von der Datenbearbeitung betroffen sind.

<sup>890</sup> BGE 136 II 508, Erw. 6.3.3; SCHÄFER/DORDI, *medialex* 2011, 146 f., m.w.H.

wie auch in Bezug auf Art und Umfang der gesammelten Daten und deren Bearbeitung [führt]. Insbesondere [seien] die Speicherung und die mögliche Verwendung der Daten ausserhalb eines ordentlichen Gerichtsverfahrens nicht klar bestimmt<sup>891</sup>.

Entgegen der Ansicht der Vorinstanz gelangte das Bundesgericht zum Schluss, dass das Interesse der Rechteinhaber „an der wirksamen Bekämpfung von Urheberrechtsverletzungen die Tragweite der Persönlichkeitsverletzung und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen [vermag]“<sup>892</sup> und hiess die Beschwerde des EDÖB gut.

Die Logistep AG verlegte daraufhin ihren Sitz sowie ihre Tätigkeit nach Deutschland. Das Oberlandgericht Hamburg entschied wenige Wochen nach dem Urteil des Bundesgerichts, dass die Tätigkeit der Logistep AG nicht gegen deutsches Recht verstossen würde, da die gesammelten *IP-Adressen* nicht als Personendaten zu qualifizieren seien.<sup>893</sup>

**b) *Rechtslage nach dem Logistep-Entscheid gemäss dem EDÖB***

Im Nachgang zum Logistep-Entscheid hielt der EDÖB in einer Mitteilung<sup>894</sup> fest, dass das Sammeln von *IP-Adressen* weiterhin möglich sei, sofern sichergestellt sei, dass:

- die Datenerhebung und -speicherung nicht über das hinausgeht, was absolut notwendig ist, um Strafanzeige gegen mutmassliche Urheberrechtsverletzer zu erstatten.
- Die Verhandlungen zwischen Rechteinhaber und (mutmasslichem) Urheberrechtsverletzer über Schadenersatzforderungen nur auf Initiative des Verletzers hin oder aber nach einer rechtskräftigen strafrechtlichen Verurteilung stattfinden.

---

<sup>891</sup> BGE 136 II 508, Erw. 6.3.3.

<sup>892</sup> BGE 136 II 508, Erw. 6.3.3.

<sup>893</sup> Urteil 5 W 126/10 des Hanseatischen Oberlandgerichts vom 3. November 2010.

<sup>894</sup> Abrufbar unter <<http://tinyurl.com/EDOEB-Mitteilung-Logistep>> (besucht 25. August 2015).

- die Rechteinhaber ihre Anstrengungen verstärken, die Beschaffung der Personendaten und den Zweck ihrer Bearbeitung für die betroffenen Personen möglichst erkennbar zu machen.

**c) *Rechtslage nach dem Logistep-Entscheid gemäss dem Entscheid des Berner Obergerichts vom 22. März 2011*<sup>895</sup>**

**aa) *Ausgangssachverhalt***

391 Die Firma „X“ ist u.a. exklusive Rechteinhaberin am Musiktitel „A“ der Künstlergruppe „Y“. Am 13. Dezember 2010 liess die Firma „X“ mit gleichzeitiger Konstituierung als Privatklägerin im Straf- und Zivilpunkt Anzeige gegen Unbekannt erstatten wegen einer Urheberrechtsverletzung i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG (unerlaubte Zugänglichmachung von Werken). Zuvor hatte die Firma „X“ eine private Firma „E“ beauftragt, die *IP-Adressen* derjenigen Personen zu ermitteln, welche das geschützte Werk „A“ über eine Tauschbörse öffentlich zugänglich gemacht hatten. Zwecks Identifikation der mutmasslichen Urheberrechtsverletzer<sup>896</sup>, beantragte die Firma „X“ bei der zuständigen Staatsanwaltschaft, es sei schnellstmöglich beim Internet-Anbieter ein entsprechendes Auskunftsgesuch zu stellen. Die Staatsanwaltschaft forderte die Firma „X“ mit Verfügung vom 7. Januar 2011 auf, einen Kostenvorschuss i.H.v. CHF 132'750.00 zu leisten und begründete dies damit, dass die beantragte Beweisführung „der Durchsetzung der Zivilklage diene und daher von der Leistung eines Kostenvorschusses [...] abhängig gemacht werden könne“. Gegen die Kostenvorschussverfügung der Staatsanwaltschaft erhob die Firma „X“ Beschwerde nach Art. 393 Abs. 1 lit. a StPO bei der Beschwerdekammer in Strafsachen des Obergerichts des Kantons Bern und machte geltend, dass die Teilnehmeridentifikation nur am Rande einer Zivilklage und zur Hauptsache der strafrechtlichen Verfolgung der Urheberrechtsverletzung dienen würde.<sup>897</sup>

**bb) *Entscheid des Berner Obergerichts***

392 Das Berner Obergericht hielt fest, dass jeweils im Einzelfall zu prüfen sei, ob die Erhebung hauptsächlich der Geltendmachung von Zivilansprüchen die-

---

<sup>895</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011 = sic! 2010, 658 ff. = CAN 2012 Nr. 36, 102 ff.

<sup>896</sup> Insgesamt wurden 531 *IP-Adressen* ermittelt.

<sup>897</sup> Vgl. zum Ganzen die Sachverhaltsdarstellung im Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 1.



nen würde. Zudem sei vorfrageweise zu klären, ob die beantragte Beweismassnahme rechtlich überhaupt zulässig sei, oder ob allenfalls ein Beweisverwertungsverbot i.S.v. Art. 141 StPO entgegensteht (Art. 139 Abs. 1 StPO). Deshalb sei es unerlässlich, „das von der Beschwerdeführerin beigebrachte Beweismittel (die ermittelten *IP-Adressen*) auf seine Rechtmässigkeit hin zu untersuchen“<sup>898</sup>. Mit Verweis auf den Logistep-Entscheid kam das Obergericht Bern zum Schluss, dass auch die von der Firma „E“ im Auftrag der Firma „X“ ermittelten *IP-Adressen*, als widerrechtlich erlangt zu gelten haben.<sup>899</sup>

Zur Frage nach der Verwertbarkeit von Beweismitteln, die von Privaten<sup>393</sup> rechtswidrig beschafft worden sind, konstatierte das Gericht zutreffend, dass hierfür in der StPO eine entsprechende Regelung fehlt.<sup>900</sup> Auch kennt die StPO keinen *numerus clausus* der Beweismittel, sondern lässt sämtliche nach dem Stand der Wissenschaft geeigneten und rechtlich zulässigen – d.h. grundrechtskonformen – Beweismittel zu.<sup>901</sup> Da die Ermittlung von *IP-Adressen* (welche gemäss bundesgerichtlicher Rechtsprechung als Personen-daten zu qualifizieren sind) einen Eingriff in die verfassungsmässige Garantie der Privatsphäre (Art. 13 Abs. 2 BV) darstellt und somit ein Grundrecht tangiert, bedarf es für die entsprechende Verfahrenshandlung – so die Argumentation des Berner Obergerichts – u.a. einer genügenden gesetzlichen Grundlage sowie eines hinreichenden Tatverdachts (Art. 197 Abs. 1 lit. a und b StPO).<sup>902</sup> Eine solche gesetzliche Grundlage für die Sammlung von *IP-Adressen* in *P2P-Netzwerken* existiert aber nach Ansicht des Berner Obergerichts gerade nicht<sup>903</sup>:

- Die Bestimmungen über die verdeckte Ermittlung seien i.c. nicht einschlägig, da bereits die Voraussetzung des „Kontakte-Knüpfs“ fehlt. Auch die übrigen Voraussetzungen zur Durchführung der verdeckten Ermittlung seien vorliegend nicht erfüllt.<sup>904</sup>

---

<sup>898</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.2.

<sup>899</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.2.

<sup>900</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.3.

<sup>901</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.4.

<sup>902</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.4.

<sup>903</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.4.; vgl. auch WULLSCHLEGER, Rz. 121 ff.

<sup>904</sup> Zu den Voraussetzungen für die Durchführung einer verdeckten Ermittlung vgl. DONATSCH/SCHWARZENEGGER/WOHLERS, 241 f.; Vorliegend fehlt die zur Durchführung der verdeckten Ermittlung erforderliche Katalogtat nach Art. 286 Abs. 2 lit. a-g URG.

- Art. 14 Abs. 4 BÜPF sei vorliegend nicht anwendbar, da nach dem Wortlaut dieser Bestimmung „die Pflicht [besteht], Angaben zur Identifikation einer Person zu machen, wenn eine Straftat über das Internet begangen wird, nicht aber zur Prüfung der Frage, ob Straftaten begangen werden (genau dazu diene aber die von der Firma E verwendete Software)“<sup>905</sup>.
- Auch die bloss „Rechtfertigung“ im Sinn von Art. 13 DSG stellt nach Ansicht des Berner Obergerichts keine genügende gesetzliche Grundlage dar.<sup>906</sup>
- Schliesslich hielt das Obergericht Bern fest, dass nicht davon ausgegangen werden könne, dass das Interesse des Staats an der Wahrheitsfindung das Interesse des Betroffenen an der Nichtverwertung des Beweises überwiegen würde, da es sich vorliegend nicht um die Aufklärung einer schweren Straftat handeln würde. „Dass das Interesse der Allgemeinheit an der Aufklärung von Urheberrechtsverletzungen nicht besonders gross ist, zeigt der Umstand, dass diese Delikte als Antragsdelikt ausgestaltet worden sind; daran ändert ein unter Umständen der Urheberrechtsinhaberin zugefügter hoher Schaden nichts“<sup>907</sup>.

**d) *Rechtslage nach dem Logistep-Entscheid gemäss dem Entscheid des Zürcher Obergerichts vom 3. Februar 2014***<sup>908</sup>

**aa) *Ausgangssachverhalt***

- 394 Die Schweizer Landesgruppe der International Federation of the Phonographic Industry (nachfolgend IFPI Schweiz) erstattete am 7. Januar 2013 Strafanzeige gegen Unbekannt wegen verschiedener Urheberrechtsverletzungen. Im Unterschied zur Sachlage beim Urteil des Berner Obergerichts<sup>909</sup>, wo sich das Auskunftsbeglehen auf die Identifizierung von insgesamt 531 *IP-Adressen* erstreckte, richtete sich die Strafanzeige der IFPI gegen einen ein-

---

<sup>905</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.4.

<sup>906</sup> Kritisch WULLSCHLEGER, Rz. 122, m.w.H.

<sup>907</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.5.

<sup>908</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014 = ZR 113/2014, 34.

<sup>909</sup> S.o. Rz. 392 f.

zelenen mutmasslichen Urheberrechtsverletzter, über dessen *IP-Adresse* beim Schweizer Internet-Anbieter „A“ zu einem bestimmten Zeitpunkt insgesamt 1'482 Musiktitel von in- und ausländischen Interpreten – ohne Einwilligung der Rechteinhaber – unerlaubt zugänglich gemacht wurden.<sup>910</sup>

Mit Verfügung vom 4. März 2013 stellte die Staatsanwaltschaft Zürich die 395 Strafuntersuchung gegen Unbekannt mit der Begründung ein, dass die zur Ermittlung der *IP-Adressen* beauftragte Firma MarkMonitor die fragliche *IP-Adresse* unter Verletzung des Datenschutzrechts ermittelt habe. Deshalb sei die ermittelte *IP-Adresse* nicht verwertbar.<sup>911</sup> Gegen diese Einstellungsverfügung erhob die IFPI Schweiz am 28. März 2013 Beschwerde bei der III. Strafkammer des Obergerichts des Kantons Zürich und stellte den Antrag, die Einstellungsverfügung sei aufzuheben und die Vorinstanz anzuweisen, die Untersuchung fortzusetzen.

*bb) Entscheidung des Zürcher Obergerichts*

Am 3. Februar 2014 urteilte das Obergericht des Kantons Zürich über die 396 Beschwerde der IFPI Schweiz gegen die Staatsanwaltschaft und hielt fest, dass das Bundesgericht die Frage nach der Verwendung von Beweisen, die unter Verletzung des Datenschutzgesetzes erhoben wurden, offen gelassen habe.<sup>912</sup> Mit Verweis auf die Lehre und die bundesgerichtliche Rechtsprechung seien die von Privaten rechtswidrig erlangten Beweismittel verwertbar, wenn sie auch von den Strafbehörden hätten erlangt werden können und kumulativ eine Interessenabwägung für deren Verwertung spricht.<sup>913</sup> Der Grundsatz *in dubio pro duriore* besagt, dass eine Einstellung des Verfahrens nur dann in Betracht kommt, wenn die Unverwertbarkeit der Beweise offensichtlich ist.<sup>914</sup> Dasselbe gilt auch bei Zweifeln über die Verwertbarkeit von

---

<sup>910</sup> EGLI, Jusletter vom 25. August 2014, Rz. 31.

<sup>911</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 2.1.; SECO, Roundtable zum Urheberrecht, 6.

<sup>912</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 4.2.

<sup>913</sup> Urteil 6B\_323/2013 vom 3. Juni 2013 des Bundesgerichts vom 3. Juni 2013, Erw. 3.4; GODENZI, 264 ff.

<sup>914</sup> BGE 138 IV 86, Erw. 4.1.1; WULLSCHLEGER, Rz. 125, weist darauf hin, „dass bei Zweifeln über die Verwertbarkeit von Beweisen das Strafverfahren trotzdem weiterzuführen ist, um den Entscheid über die Verwertbarkeit der Beweise und die damit verbundene Interessenabwägung dem Sachgericht zu überlassen; WOHLERS, FP 2011, 370.

Beweismitteln.<sup>915</sup> Sodann hielt das Obergericht Zürich fest, dass im vorliegenden Fall nicht zweifelsfrei verneint werden könne, ob nicht bereits vor der Datenerhebung durch MarkMonitor Hinweise vorlagen, aufgrund derer die IFPI eine Strafanzeige hätte erheben können. Diesfalls wäre die Staatsanwaltschaft gestützt auf Art. 309 Abs. 1 lit. a StPO befugt gewesen, selber Beweise zu erheben. Nach Ansicht des Zürcher Obergerichts sprechen diese Zweifel gegen eine Einstellung des Strafverfahrens.<sup>916</sup> Weiter gab das Obergericht zu bedenken, dass die Frage nach der Verwertbarkeit illegal beschaffter Beweise durch Private von einer Abwägung der Interessen an der Strafverfolgung und am Persönlichkeitsschutz abhängig sei.<sup>917</sup> Das Obergericht kam zum Schluss, dass sich die Sach- und Rechtslage betreffend die Frage nach der Verwertbarkeit der unter Verletzung des DSG beschafften Beweise als unklar erweisen würde und eine „Einstellung des Strafverfahrens den Grundsatz «im Zweifel für die Anklageerhebung» (Art. 5 Abs. 1 BV und Art. 2 Abs. 1 StPO in Verbindung mit Art. 319 Abs. 1 und Art. 324 Abs. 1 StPO) [verletzen würde]“<sup>918</sup>. Folglich hiess das Zürcher Obergericht die Beschwerde der IFPI gut, ordnete die Aufhebung der Einstellungsverfügung an und wies die Sache zur Fortsetzung des Verfahrens an die Staatsanwaltschaft zurück.<sup>919</sup>

## **B. Kritische Würdigung der Rechtslage beim Sammeln von *IP-Adressen de lege lata***

### **a) *IP-Adressen als Personendaten i.S.v. Art. 3 lit. a DSG***

- <sup>397</sup> Das Bundesgericht hielt im Logistep-Entscheid fest, dass die Qualifikation von *IP-Adressen* als Personendaten i.S.v. Art. 3 Abs. 1 lit. a DSG nicht abstrakt festgestellt werden könne, sondern immer „vor dem Hintergrund der

---

<sup>915</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 5.2 mit Verweis auf den Entscheid BB.2012.148 des Bundesstrafgerichts vom 10. April 2013, Erw. 2.1.

<sup>916</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 5.3; EGLI, Jusletter vom 25. August 2014, Rz. 32.

<sup>917</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 5.3 mit Verweis auf BGE 136 II 508, Erw. 6.3.

<sup>918</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 5.4.

<sup>919</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 6.

konkreten Umstände des Einzelfalls<sup>920</sup> aus der Sicht des jeweiligen Inhabers der Information zu beurteilen sei.<sup>921</sup> Im konkreten Fall beurteilte das Bundesgericht, dass sowohl statische wie auch dynamische *IP-Adressen*<sup>922</sup> als Personendaten i.S.v. Art. 3 Abs. 1 lit. a DSG zu qualifizieren seien, da die Identität des Anschlussinhabers ohne unverhältnismässigen Aufwand bestimmbar sei, wobei es bereits genügt, falls die mutmasslichen Urheberrechtsverletzer nach Übergabe der entsprechenden Daten an die Strafverfolgungsbehörde für die Rechteinhaber (aufgrund der Information selbst oder aufgrund von diesen zugänglichen Zusatzinformationen) bestimmbar werden.<sup>923</sup> PROBST kritisiert an dieser Auslegung, dass es für eine globalisierte Informationsgesellschaft kein tragfähiges Konzept darstellen würde, wenn an sich anonyme Daten automatisch als Personendaten qualifiziert werden, sobald diese durch die blosser Weitergabe an einen oder mehrere nachgelagerte Datenempfänger (infolge Verknüpfung mit zusätzlichen Daten) in einem Einzelfall die Bestimmbarkeit einer einzigen betroffenen Person ermöglicht.<sup>924</sup> Diese Problematik ist insoweit zu relativieren, als auf dem Gebiet der wissenschaftlichen Forschung, Planung und Statistik mit Art. 13 Abs. 2 lit. e DSG bereits eine Ausnahmeregelung existiert, welche die Bearbeitung von Personendaten zu nicht personenbezogenen Zwecken regelt, sofern die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

**b) *Persönlichkeitsverletzung nach Art. 12 Abs. 2 lit. a DSG***

In seinem Urteil bestätigte das Bundesgericht den Entscheid der Vorinstanz, wonach die Datenbearbeitung der Logistep AG gegen die Grundsätze der Zweckbindung und der Erkennbarkeit (Art. 4 Abs. 3 und Abs. 4 DSG)

---

<sup>920</sup> BGE 136 II 508, Erw. 3.5.

<sup>921</sup> BGE 136 II 508, Erw. 3.4 f.; WULLSCHLEGER, Rz. 48 ff.; ROSENTHAL, *digma* 2011, 41.

<sup>922</sup> Wird einem Rechner eine *IP-Adresse* fest zugewiesen, spricht man von einer statischen oder festen *IP-Adresse*. Erhält ein Nutzer bei jeder Verbindungsaufnahme eine neue (freie) *IP-Adresse* aus dem Pool des Providers zugewiesen, spricht man von einer dynamischen *IP-Adresse*; ausführlich dazu WULLSCHLEGER, Rz. 27 ff.; WEBER/FERCSIK SCHNYDER, *sic!* 2009, 579 f.; ROSENTHAL, *digma* 2011, 40.

<sup>923</sup> BGE 136 II 508, Erw. 3.4.; WULLSCHLEGER, Rz. 59 ff.; SCHÄFER/DORDI, *medialex* 2011, 142; ROSENTHAL, *digma* 2011, 41; a.A. PROBST, *AJP* 2013, 1429 f.; GLARNER/RÜFENACHT, *Jusletter* vom 20. Dezember 2010, Rz. 8, die darauf verweisen, dass *IP-Adressen* „nur über die Identität der Zugangsinhaber, nicht [aber] über die Identität des effektiven Zugangsnutzers Auskunft geben“.

<sup>924</sup> PROBST, *AJP* 2013, 1430, 1435 f.

verstösst.<sup>925</sup> Diese Feststellung des Bundesgerichts ist nicht zu beanstanden, da weder die Aufzeichnung der *IP-Adressen* noch der Zweck der Bearbeitung für die betroffenen Personen ersichtlich war, weshalb nach Art. 12 Abs. 2 lit. a DSG *per se* eine Verletzung der Persönlichkeit vorliegt.<sup>926</sup>

### c) *Rechtfertigungsgründe*

- 399 Das Bundesgericht hielt in seinem Entscheid fest, dass eine Einwilligung der Betroffenen oder eine Rechtfertigung durch Gesetz ganz offensichtlich verneint werden müsse, weshalb einzig ein überwiegendes privates oder öffentliches Interesse in Betracht kommt.<sup>927</sup> WULLSCHLEGER bringt diesbezüglich vor, „dass auch die Durchsetzung und Verwirklichung des Urheberrechts im öffentlichen Interesse liegt“<sup>928</sup>. Dessen ungeachtet stellte das Bundesgericht klar, dass eine Rechtfertigung der durch den Verstoss gegen die Bearbeitungsgrundsätze nach Art. 4, Art. 5 Abs. 1 und Art. 7 DSG verursachten Persönlichkeitsverletzung „zwar nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall aber nur mit grosser Zurückhaltung bejaht werden können“<sup>929, 930</sup>.
- 400 Indem das Bundesgericht – zu Ungunsten der Rechteinhaber – zum Schluss gelangte, dass vorliegend „das Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen die Tragweite der Persönlichkeitsverletzung und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen [vermag]“<sup>931</sup>, wurde der in Art. 13 Abs. 1 DSG verankerte Mechanismus zum Ausgleich der Interessen, zumindest im Bereich der Ermittlung von *IP-Adressen* zum Zwe-

---

<sup>925</sup> BGE 136 II 508, Erw. 6.3.1; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 11; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 4, der die Frage aufwirft, ob jemand, der eine Werkkopie unerlaubt über das Internet zugänglich macht, tatsächlich nicht damit rechnen muss, dass ein Rechteinhaber – sofern er ihn dabei ertappt – seine *IP-Adresse* und weitere relevante Daten aufzeichnet. Vgl. dazu auch THOUVENIN, Big Data, 63 ff., mit einer ausführlichen Analyse zu den Grundsätzen der Zweckbindung und der Erkennbarkeit.

<sup>926</sup> ROSENTHAL, Jusletter vom 27. September 2010, Rz. 4.

<sup>927</sup> BGE 136 II 508, Erw. 6.3.1.

<sup>928</sup> WULLSCHLEGER, Rz. 103.

<sup>929</sup> BGE 136 II 508, Erw. 5.2.4.

<sup>930</sup> Vgl. SCHÄFER/DORDI, medialex 2011, 142 f., m.w.H.; ROSENTHAL, digma 2011, 41; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 12; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 5.

<sup>931</sup> BGE 136 II 508, Erw. 6.3.3.

cke der Verfolgung von Urheberrechtsverletzungen, faktisch ausser Kraft gesetzt.<sup>932</sup>

## 2. Neue gesetzliche Grundlagen für die Ermittlung der Täterschaft bei Urheberrechtsverletzungen im Internet *de lege ferenda*

Das Bundesgericht hält in seinem Urteil fest, dass es Sache des Gesetzgebers und nicht des Richters sei, die allenfalls notwendigen Massnahmen zu treffen, um einen den neuen Technologien entsprechenden Urheberrechtsschutz zu gewährleisten.<sup>933</sup> In ihrem Schlussbericht spricht sich die AGUR12 dafür aus, dass die Rechteinhaber „für die Ermittlung von Urheberrechtsverletzungen Internetverbindungsdaten (insbesondere dynamische und statische *IP-Adressen*) bearbeiten dürfen [sollen], soweit sie sich an die Vorgaben des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) halten. Die gesetzlichen Grundlagen [seien] – soweit erforderlich – zu schaffen“<sup>934</sup>.

ROSENTHAL und THOUVENIN halten dieser Ansicht m.E. zu Recht entgegen, dass Privatpersonen für die Bearbeitung von Personendaten keine gesetzliche Grundlage benötigen.<sup>935</sup> Dem Erfordernis einer expliziten gesetzlichen Grundlage im Zuge einer Gesetzesrevision kann sodann entgegengehalten

---

<sup>932</sup> Ebenso THOUVENIN, ACTA, 113 f., der davon ausgeht, dass eine effiziente Verfolgung von Urheberrechtsverletzungen durch den *Upload* geschützter Werke in *P2P-Netzwerken* in der Schweiz an den Vorgaben des Datenschutzes scheitert; vgl. auch WULLSCHLEGER, Rz. 126 f., 430 f., nach dessen Ansicht eine Bearbeitung von *IP-Adressen* zwar weiterhin möglich ist, aber eine Durchsetzung gegenüber den Urheberrechtsverletzern scheitert, weil die Privaten ihre Datenbearbeitung nicht formell durch den EDÖB genehmigen lassen können. Dadurch bleiben die Rechteinhaber im Unklaren, ob die erhobenen *IP-Adressen* im Einzelfall als Beweismittel für eine Urheberrechtsverletzung dienen können. Sodann weist der Autor auf die Gefahr hin, dass die Behörden bei sämtlichen systematischen Ermittlungen durch die Rechteinhaber von einem gleichgelagerten Fall wie im *Logistep-Entscheid* ausgehen und auf ein Beweisverwertungsverbot schliessen; SECO, Roundtable zum Urheberrecht, 4.

<sup>933</sup> BGE 136 II 508, Erw. 6.4; vgl. dazu auch ROSENTHAL, *digma* 2011, 41, wonach dieser Nachsatz „dem kritischen Beobachter jedoch eher als Rechtfertigung für einen Fehlentscheid als ein ernsthafter Aufruf zur Gesetzesrevision erscheinen [mag]“.

<sup>934</sup> AGUR12, Schlussbericht, 75.

<sup>935</sup> THOUVENIN, *Big Data*, 77; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 15; Eine gesetzliche Grundlage ist gem. Art. 17 Abs. 1 DSGVO nur für die Bearbeitung von Personendaten durch Bundesorgane erforderlich.

werden, dass mit der in Art. 13 Abs. 1 DSG verankerten Möglichkeit zur Interessenabwägung und dem Auskunftsanspruch nach Art. 14 Abs. 4 BÜPF bereits Bestimmungen vorhanden sind, die eine Rechtsdurchsetzung auch bei von Privaten erhobenen Beweisen ermöglichen.<sup>936</sup>

- 403 Wie ROSENTHAL zutreffend vorbringt, werden die aufgezeichneten *IP-Adressen* überhaupt erst dadurch zu Personendaten i.S.v. Art. 3 Abs. 1 lit. a DSG, weil Art. 14 Abs. 4 BÜPF die Internetanbieter verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Inhabers ermöglichen, über dessen Internetanschluss eine strafbare Handlung begangen worden ist.<sup>937</sup> Entgegen der Feststellung des Berner Obergerichts dient die zur Ermittlung der *IP-Adressen* eingesetzte Software nicht zur Aufklärung, ob eine strafbare Handlung stattgefunden hat. Dass eine Urheberrechtsverletzung vorliegt, steht bereits im Zeitpunkt fest, in dem *P2P-Nutzer* aus der Schweiz ein geschütztes Werk ohne Einwilligung der Rechteinhaber im Internet öffentlich zugänglich machen (Art. 67 Abs. 1 lit. g<sup>bis</sup> URG).<sup>938</sup> Die Software dient lediglich zur Sicherstellung von Beweismitteln für ein nachfolgendes straf- bzw. zivilrechtliches Verfahren gegen die mutmasslichen Urheberrechtsverletzer, indem die *IP-Adressen* derjenigen Nutzer aufgezeichnet werden, die sich über eine *IP-Adresse* aus der Schweiz an einem *P2P-Netzwerk* beteiligen und dabei urheberrechtlich geschützte Werke unerlaubt zugänglich machen.
- 404 Zutreffend bemerkte das Zürcher Obergericht, dass die Staatsanwaltschaft nicht zweifelsfrei nachweisen konnte, ob nicht bereits vor der softwareunterstützten Aufzeichnung der *IP-Adressen* Hinweise vorlagen, aufgrund derer eine Strafanzeige hätte gestellt werden können.<sup>939</sup> So hätte die beauftragte Firma beispielsweise auch ohne vorgängige Aufzeichnung der *IP-Adresse* den *Link* zum Bezug der *P2P-Software* mit Angabe des unerlaubt darüber zugänglich gemachten Werks bzw. die *.torrent-Datei* zum *Download* des Werks an die Staatsanwaltschaft übermitteln und Strafanzeige gegen Unbekannt erstatten können.<sup>940</sup> Gestützt auf Art. 309 Abs. 1 lit. a StPO hätte die

---

<sup>936</sup> ROSENTHAL, *digma* 2011, 41; ders., Jusletter vom 27. September 2010, Rz. 12.

<sup>937</sup> SCHWEIZER/BISCHOF, *digma* 2011, 154; GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 16; ROSENTHAL, Jusletter vom 27. September 2010, Rz. 14.

<sup>938</sup> Entscheid des Obergerichts des Kantons Bern, BK 11 9, vom 22. März 2011, Erw. 2.4.

<sup>939</sup> Entscheid UE130087 des Obergerichts des Kantons Zürich vom 3. Februar 2014, Erw. 5.3.

<sup>940</sup> Diese Hinweise begründen m.E. einen hinreichenden Tatverdacht auf Urheberrechtsverletzungen i.S.v. Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG.



Zürcher Staatsanwaltschaft auch ohne vorgängige Übermittlung der *IP-Adressen* eine Untersuchung eröffnen und die *IP-Adressen* selbst erheben bzw. durch einen Dritten erheben lassen können. Es erscheint allerdings wenig sinnvoll, die Ermittlung von *IP-Adressen* an die Staatsanwaltschaft zu delegieren, da diese weder über die erforderlichen Ressourcen verfügt noch genügend zeitnah operieren kann.<sup>941</sup> Es sprechen somit auch praktische Gründe dafür, dass die Rechteinhaber bzw. von diesen beauftragte Dritte – nach erfolgter Feststellung von Urheberrechtsverletzungen über *Filesharing*-Netzwerke – die *IP-Adressen* der Teilnehmer selbst aufzeichnen dürfen.<sup>942</sup>

GLARNER/RÜFENACHT kommen in ihrer Publikation u.a. zum Ergebnis, dass eine Durchsetzung der Urheberrechte selbst dann nicht verunmöglicht werde, „wenn die aus Schweizer Optik datenschutzwidrig beschafften Daten einem Beweisverwertungsverbot unterliegen“, da die Rechteinhaber weiterhin über das Akteneinsichtsrecht in der Strafuntersuchung Kenntnis vom mutmasslichen Urheberrechtsverletzer nehmen und anschliessend ihre Interessen gegen diesen auf dem Zivilweg geltend machen könnten.<sup>943</sup> Diese Ansicht blendet jedoch die Tatsache aus, dass die Staatsanwaltschaften seit dem Logistep-Entscheid regelmässig von der Einleitung einer Strafuntersuchung absehen, falls die *IP-Adressen* unter Verletzung des Datenschutzrechts erhoben worden sind.<sup>944</sup> Schliesslich ist auch Art. 152 Abs. 2 ZPO zu beachten, wonach rechtswidrig beschaffte Beweismittel nur berücksichtigt werden, wenn das Interesse an der Wahrheitsfindung überwiegt.

Die Entscheide der Obergerichte der Kantone Bern und Zürich zeigen auf, dass seit dem Logistep-Entscheid hinsichtlich der Zulässigkeit der Aufzeichnung von *IP-Adressen* durch die Rechteinhaber eine erhebliche Rechtsunsicherheit besteht. Anstatt den Logistep-Entscheid lediglich als Einzelfallurteil und Fehlentscheid abzutun, erscheint es deshalb notwendig, eine konkrete gesetzliche Grundlage für die Datenbearbeitung zur Verfolgung von Urheberrechtsverletzungen im Internet zu schaffen.<sup>945</sup> Da es sich um ein datenschutzrechtliches Problem handelt, sollte dieses sinnvollerweise im DSG

---

<sup>941</sup> So auch WULLSCHLEGER, Rz. 433, wonach Einschränkungen bei der Bearbeitung nicht dazu führen sollen, „dass einem Strafantrag wegen einer im Internet begangenen Urheberrechtsverletzung anhand von rudimentären Hinweisen nachgegangen wird“.

<sup>942</sup> Vgl. WULLSCHLEGER, Rz. 433; AGUR12, Schlussbericht, 75.

<sup>943</sup> GLARNER/RÜFENACHT, Jusletter vom 20. Dezember 2010, Rz. 22.

<sup>944</sup> Vgl. WULLSCHLEGER, Rz. 125; SECO, Roundtable zum Urheberrecht, 4.

<sup>945</sup> Ebenso WULLSCHLEGER, Rz. 432.

geregelt werden.<sup>946</sup> Um die gegenwärtige Rechtsunsicherheit im Umgang mit den von Privaten gesammelten *IP-Adressen* zu beseitigen, wird deshalb vorgeschlagen, in einem neuen Art. 13 Abs. 2 lit. g DSG detailliert und unter Berücksichtigung der Vorgaben des EDÖB festzuhalten, welche Anforderungen erfüllt sein müssen, damit ein überwiegendes Interesse der bearbeitenden Person bejaht werden kann.<sup>947</sup>

**Art. 13 Abs. 2 lit. g DSG (Neuregelung) - Rechtfertigungsgründe**

<sup>2</sup> Ein überwiegendes Interesse der bearbeitenden Person fällt insbesondere in Betracht, wenn diese:

*Daten über die Inhaber von Internetzugängen zum Zwecke der zivil- bzw. strafrechtlichen Verfolgung bearbeitet, sofern deren Internetzugänge zur Begehung von Urheberrechtsverletzungen genutzt werden. Die Rechteinhaber sind verpflichtet auf ihren Webseiten detailliert Auskunft über die Vorgehensweise sowie die Art und den Umfang der gesammelten Daten zu geben.*

- 407 Damit sichergestellt werden kann, dass die Rechteinhaber ihre Schadenersatzansprüche gegenüber den fehlbaren Nutzern erst nach einer rechtskräftigen strafrechtlichen Verurteilung bzw. auf Initiative der betroffenen Nutzer hin geltend machen, ist darüber hinaus eine Anpassung der reparatorischen Ansprüche nach Art. 62 Abs. 2 URG vorzunehmen:

---

<sup>946</sup> Siehe dazu auch SECO, Roundtable zum Urheberrecht, 7; A.A. WULLSCHLEGER, Rz. 435 ff., plädiert für die Einführung eines verletzungsunabhängigen Auskunftsanspruchs im Fernmeldegesetz, da dieses gem. Art. 1 Abs. 2 lit. b FMG einen die „Immaterialgüterrechte achtenden Fernmeldeverkehr sicherstellen“ soll.

<sup>947</sup> RUDIN, *digma* 2011, 145, der zur Modernisierung des Datenschutzrechts ausführt, dass diese auf zwei Arten erfolgen kann: „Indem man entweder den Begriff der Personendaten enger macht und damit weite Bereiche von Datenbearbeitungen aus dem Datenschutzrecht „entlässt“, oder indem man die Rechtfertigungstatbestände [...] neu diskutiert und allenfalls anpasst“; Alternativ zur nachfolgend skizzierten Anpassung der Rechtfertigungstatbestände nach Art. 13 DSG, hätte auch die in Art. 3 lit. a DSG statuierte Begriffsdefinition der Personendaten eingeschränkt werden können, indem explizit im Gesetz festgehalten wird, dass *IP-Adressen* nicht als Personendaten i.S.d. DSG zu qualifizieren sind. Dadurch würde die Unsicherheit in Bezug auf die angewendeten Methoden zur Datensammlung sowie die Art und den Umfang der gesammelten Daten und deren Bearbeitung nicht beseitigt. Weitere Unklarheiten bestehen mit Blick auf die Speicherung der Daten sowie eine mögliche Verwendung ausserhalb eines ordentlichen Gerichtsverfahrens. In Anbetracht dieser Unsicherheiten ist die Anpassung der Rechtfertigungstatbestände nach Art. 13 DSG gegenüber einer Ausklammerung der *IP-Adressen* aus der Begriffsdefinition der Personendaten gem. Art. 3 lit. a DSG zu bevorzugen.

**Art. 62 Abs. 2 URG (Ergänzungsvorschlag) - Leistungsklagen**

<sup>2</sup> Vorbehalten bleiben die Klagen nach dem Obligationenrecht auf Schadenersatz, auf Genugtuung sowie auf Herausgabe eines Gewinns entsprechend den Bestimmungen über die Geschäftsführung ohne Auftrag. *Schadenersatzansprüche bei Urheberrechtsverletzungen im Internet bei denen der mutmassliche Urheberrechtsverletzer durch Aufzeichnung der IP-Adresse ermittelt wurde, können nur auf Initiative der beschuldigten Person hin oder nach einer rechtskräftigen strafrechtlichen Verurteilung geltend gemacht werden.*

## II. Warnhinweismodell

### 1. Vorschlag der AGUR12

In ihrem Schlussbericht schlägt die AGUR12 die Einführung eines Warnhinweismodells vor<sup>948</sup>: Die *Access-Provider* sollen auf Hinweis der Rechteinhaber oder einer zuständigen Behörde einen einmaligen aufklärenden Hinweis an die Inhaber von Internetanschlüssen versenden, über welche *P2P-Netzwerke* genutzt und dabei „in schwerwiegender Weise“ Urheberrechte verletzt wurden. Die *Access-Provider* sollen für ihren Aufwand eine angemessene Vergütung von den Rechteinhabern erhalten. Durch den Hinweis soll der betroffene Anschlussinhaber über sein eigenes Fehlverhalten bzw. über das Fehlverhalten der seinen Internetanschluss (mit-)benützenden Personen informiert werden.<sup>949</sup> Zur Verhinderung einer zivilrechtlichen Mithaftung im Wiederholungsfall ist der Anschlussinhaber verpflichtet, „den Weitergebrauch seines Anschlusses für Rechtsverletzungen über *P2P-Netzwerke* in angemessener Weise zu schützen“<sup>950</sup>.

---

<sup>948</sup> Vgl. AGUR12, Schlussbericht, 75; WULLSCHLEGER, Rz. 316, mit ausführlichen Hinweisen zum Grundkonzept der sog. *Graduated Response Systemen*.

<sup>949</sup> Bspw. durch Familienmitglieder, Mitbewohner einer Wohngemeinschaft oder fremde Nutzer bei öffentlichen WLAN-Hotspots.

<sup>950</sup> AGUR12, Schlussbericht, 75.

## 2. Bisherige Erfahrungen mit einem Warnhinweismodell am Beispiel Frankreichs

- 409 In Frankreich wurde im Jahr 2009 mit den beiden sog. HADOPI-Gesetzen und den dazugehörigen Verordnungen ein Warnhinweismodell zur Bekämpfung von Urheberrechtsverletzungen im Internet eingeführt.<sup>951</sup> Grundlage bildete ein dreistufiges Warnhinweisverfahren<sup>952</sup>, welches von der neu eingerichteten staatlichen Behörde HADOPI<sup>953</sup> durchgeführt wurde.<sup>954</sup> Zur Ermittlung der Urheberrechtsverletzungen wurden private Firmen<sup>955</sup> von den Rechteinhabern beauftragt. Diese erstellten ein Protokoll des Urheberrechtsverstosses samt den dazugehörigen *IP-Adressen* der betroffenen Anschlussinhaber.<sup>956</sup>
- 410 Die Anschlussinhaber, über deren *IP-Adressen* eine Urheberrechtsverletzung ermittelt wurde, erhielten von ihren *Access-Providern* einen ersten Warnhinweis via E-Mail zugestellt.<sup>957</sup> Wurde binnen sechs Monaten seit Versand des ersten Warnhinweises erneut eine Urheberrechtsverletzung festgestellt, wurde dem Anschlussinhaber ein zweiter Warnhinweis mittels eines Einschreibens zugestellt, worin dieser dazu verpflichtet werden konnte, gewisse Sicherheitsmassnahmen zu treffen.<sup>958</sup>

---

<sup>951</sup> Ausführlich dazu WULLSCHLEGER, Rz. 326 ff.; vgl. auch THOUVENIN, ACTA, 117 ff., m.w.H. zu den sog. *Graduated Response Systemen*; GESMANN-NUSSL/WÜNSCHE, GRUR-Int. 2012, 231; SCHWARTMANN, GRUR-Prax 2012, 159; GEIGER, IIC 2011, 458; SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298; Loi n° 2009-669 vom 12. Juni 2009 „Loi favorisant la diffusion et la protection de la création sur internet“ (sog. HADOPI 1-Gesetz), abrufbar unter <<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432>> (besucht 25. August 2015) und Loi n° 2009-1311 vom 28. Oktober 2009 „Loi relative à la protection pénale de la propriété littéraire et artistique sur internet“ (sog. HADOPI 2-Gesetz), abrufbar unter <<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&categorieLien=id>> (besucht 25. August 2015).

<sup>952</sup> „Three Strikes“-Modell, SCHWARTMANN, GRUR-Prax 2012, 159.

<sup>953</sup> Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet.

<sup>954</sup> SCHWARTMANN, GRUR-Prax 2012, 159; GEIGER, IIC 2011, 458; SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298.

<sup>955</sup> Wie etwa Trident Media Guard (TMG), <[www.tmg.eu](http://www.tmg.eu)> (besucht 25. August 2015).

<sup>956</sup> Vgl. zum Ganzen SCHWARTMANN, GRUR-Prax 2012, 159;

<sup>957</sup> SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298, welche auf die Schwächen der Zustellung eines ersten Warnhinweises via E-Mail eingehen. Dabei wird insbesondere auch auf die Gefahr des Phishings hingewiesen; vgl. auch BENABOU, 171.

<sup>958</sup> BENABOU, 173 f.; STROWEL, 149 f.

Falls innerhalb des darauffolgenden Jahres ein weiterer Urheberrechtsverstoss festgestellt wurde, konnte die HADOPI den Sachverhalt an die zuständige Staatsanwaltschaft übergeben, die sodann gestützt auf den Abschlussbericht der HADOPI ein Strafverfahren einleiten konnte.<sup>959</sup> Wenn der Anschlussinhaber die Urheberrechtsverletzungen selbst begangen hat, drohen diesem bis zu drei Jahren Gefängnis und EUR 300'000 Busse.<sup>960</sup> Falls der Anschlussinhaber eine Urheberrechtsverletzung zwar nicht selbst begangen, jedoch in fahrlässiger Weise unterstützt hat, kann dieser mit einer einmonatigen Internetzugangssperre sowie mit einer Busse bis zu EUR 3'750 bestraft werden.<sup>961</sup> 411

Obschon im Zeitraum von Oktober 2010 bis Juni 2013 über 1,2 Mio. Warnhinweise wegen Urheberrechtsverletzungen von der HADOPI versendet worden sind, wurden nur gerade drei Gerichtsverfahren mit einem Urteil abgeschlossen, wovon eines mit Geldstrafe von EUR 150, eines mit einer Verwarnung und eines mit einem Freispruch endete.<sup>962</sup> Angesichts der beachtlichen Kosten<sup>963</sup>, dem marginalen Erfolg sowie den Konflikten dieser Praxis mit dem Datenschutz hält HOEREN das von der HADOPI angewendete Three-Strikes-Modell für gescheitert.<sup>964</sup> 412

### 3. Kritische Würdigung der Einführung eines Warnhinweismodells

Der Vorschlag, welcher den harmlosen Titel „Aufklärende Hinweise“ trägt, ist m.E. als sehr problematisch einzustufen. Zunächst ist es höchst fraglich, ob – wie dies von der AGUR12 wiederholt behauptet wird – mit Blick auf 413

<sup>959</sup> SCHWARTMANN, GRUR-Prax 2012, 159; SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298; BENABOU, 174; STROWEL, 150.

<sup>960</sup> Art. L. 335-4 CPI; WULLSCHLEGER, Rz. 330; SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298; BENABOU, 178.

<sup>961</sup> Art. L. 335-7-1 CPI; WULLSCHLEGER, Rz. 330.

<sup>962</sup> SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298, die ebenfalls auf die wirtschaftliche Ineffizienz des Gesetzes hinweisen.

<sup>963</sup> WULLSCHLEGER, Rz. 332, mit dem Hinweis, dass sich die Kosten für die 60 HADOPI-Mitarbeiter rund EUR 13,5 Mio. betrugen.

<sup>964</sup> BECHTOLD, ZSR 2015 II, 105; HOEREN, sic! 2014, 214 f.; ähnlich SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298, die von einem „missglückten Gesetz“ sprechen; WULLSCHLEGER, Rz. 332, wonach sich die relativ hohen Betriebskosten der HADOPI ohne einen Nachweis der Wirksamkeit längerfristig „wohl kaum rechtfertigen [lassen]“.

die Nutzung von *P2P-Netzwerken* zum Austausch urheberrechtlich geschützter Werke tatsächlich davon gesprochen werden kann, dass „die Internetnutzer oftmals über die Rechtslage im Unklaren sind“. Aus einer Studie zur digitalen Content-Nutzung in Deutschland geht hervor, dass 97% der deutschen Bevölkerung, die älter als zehn Jahre alt ist, davon Kenntnis hat, dass die Nutzung von Tauschbörsen für den *Download* urheberrechtlich geschützter Medieninhalte nicht rechtmässig ist.<sup>965</sup>

- 414 Soweit ersichtlich wurde in der Schweiz bislang keine entsprechende Umfrage durchgeführt. Da die Nutzer von *P2P-Netzwerken* zumeist über laienhafte Grundkenntnisse bezüglich deren Funktionsweise verfügen, ist davon auszugehen, dass sich auch in der Schweiz nahezu sämtliche Nutzer bewusst sind, dass das Hochladen von urheberrechtlich geschützten Werken in einem *P2P-Netzwerk* gegen das schweizerische Urheberrechtsgesetz verstösst. Wird eine Aufklärung der Internetnutzer über die Rechtslage beim *Filesharing* angestrebt, kann dies auch auf anderem Wege als durch die Einführung eines Warnhinweismodells erreicht werden.<sup>966</sup>
- 415 Weiter ist am vorgeschlagenen Warnhinweismodell zu beanstanden, dass sich dieses zu einseitig nur auf Urheberrechtsverletzungen bezieht, die über *P2P-Netzwerke* begangen werden. Insbesondere die *Filehoster* (teilweise auch als *Sharehoster* oder *One-Click-Hoster*<sup>967</sup> bezeichnet) haben sich zu einer valablen Alternative zu den *P2P-Netzwerken* entwickelt.<sup>968</sup> Auch hier können urheberrechtlich geschützte Werke unerlaubt zugänglich gemacht werden. Es ist daher nicht einzusehen, weshalb das Warnhinweismodell einseitig auf *P2P-Netzwerke* beschränkt bleiben soll.
- 416 Anlass zu Kritik gibt auch die auslegungsbedürftige Formulierung, wonach Warnhinweise nur dann an die Anschlussinhaber zugestellt werden sollen, wenn bei der Nutzung der *P2P-Netzwerke* „in schwerwiegender Weise“ Urheberrechte verletzt wurden. Eine solche Regelung steht im Widerspruch zu

---

<sup>965</sup> HILGARD, I, allerdings muss die Studie mit einer gewissen Zurückhaltung interpretiert werden, da sie von der Seite der Rechteinhaber in Auftrag gegeben wurde.

<sup>966</sup> Eine entsprechende Aufklärungskampagne, die an sämtliche Internetnutzer adressiert ist (nicht nur an diejenigen, bei denen bereits schwerwiegende Urheberrechtsverletzungen registriert wurden), wäre gegenüber dem Warnhinweismodell eine weniger einschneidende Massnahme; kritisch dazu MAY, 207, welche die erzielten Effekte einer entsprechenden Kampagne in Deutschland (allerdings ohne Nachweise) als „eher bescheiden“ taxiert.

<sup>967</sup> Uploaded.net, Rapidgator.net, Bitshare.com, etc.

<sup>968</sup> WULLSCHLEGER, Rz. 363; SCHÄUFELE, 31 f., m.w.H.

Art. 67 Abs. 1 lit. g<sup>bis</sup> bzw. Art. 69 Abs. 1 lit. e<sup>ter</sup> URG, deren objektive Tatbestände bereits mit der unerlaubten öffentlichen Zugänglichmachung erfüllt sind. M.a.W. reicht für eine Strafbarkeit bereits die Möglichkeit aus, dass Dritte auf das geschützte Werk zugreifen können. Nicht erforderlich ist demgegenüber, dass das Werk tatsächlich von einem Dritten heruntergeladen wird. Dass nun bei Urheberrechtsverletzungen über das Internet zunächst bloss ein Warnhinweis zugestellt wird, ist mit der gesamten restlichen Strafrechtsordnung inkonsistent.

Unklarheit besteht m.E. auch darüber, ob der eigentliche Urheberrechtsver- 417  
 letzer (der nicht mit dem Anschlussinhaber identisch sein muss) nach Einführung des Warnhinweismodells weiterhin bestraft werden kann.<sup>969</sup> Im Vorschlag der AGUR12 werden jedenfalls nur die Anschlussinhaber adressiert und nicht die eigentlichen fehlbaren Nutzer.<sup>970</sup> Würde jedoch auf eine Strafverfolgung des Urheberrechtsverletzers verzichtet, führte dies zu einer dogmatisch nur schwer begründbaren Besserstellung derjenigen Täter, die über das Internet (*P2P-Netzwerke*) gegen das Urheberrecht verstossen haben, gegenüber jenen, die auf andere Weise eine Urheberrechtsverletzung begangen haben.<sup>971</sup> Die Privilegierung ist darin zu sehen, dass gegen Letztere ein Strafverfahren geführt wird, während die Erstgenannten beim Warnhinweismodell „mit einem blauen Auge“ davonkommen. *De lege lata* ist im Urheberstrafrecht keine Bestimmung enthalten, welche die Einstellung der Strafverfolgung durch einen aufklärenden Hinweis vorsieht. Bei einer Einführung des Warnhinweismodells müssten deshalb auch die Strafbestimmungen von Art. 67 ff. URG um einen entsprechenden Vorbehalt ergänzt werden. Überdies müsste auch der zivilrechtliche Schutz nach Art. 61 ff. URG angepasst werden, da es den Rechteinhabern ansonsten unbenommen bleibt, Schadenersatzansprüche gegen Urheberrechtsverletzer geltend zu machen.<sup>972</sup>

Der eigentliche Hauptkritikpunkt bezieht sich auf die Einführung „einer 418  
 zivilrechtlichen Mithaftung im Wiederholungsfall“ für die Anschlussinhaber. Im Vergleich zur gegenwärtigen Rechtslage, in der nur Täter und Teilnehmer

<sup>969</sup> Sofern ermittelt werden kann, welche den fraglichen Internetanschluss benutzende Person die Urheberrechtsverletzung begangen hat.

<sup>970</sup> A.A. WIGGER, UFITA II/2014, 517.

<sup>971</sup> So etwa der Verkauf oder das Verschenken von selbstgebrannten CDs/DVDs an Drittpersonen ausserhalb des Privatgebrauchs nach Art. 19 Abs. 1 lit. a URG.

<sup>972</sup> So kann sichergestellt werden, dass Schadenersatzforderungen – gemäss den Vorgaben des EDÖB – nur auf Initiative des mutmasslichen Urheberrechtsverletzers oder nach einer rechtskräftigen strafrechtlichen Verurteilung gestellt werden.

der Urheberrechtsverletzung rechtlich belangt werden können, würde *de lege ferenda* eine Kausalhaftung für die Anschlussinhaber eingeführt, falls nach Zustellung des aufklärenden Hinweises erneut Urheberrechtsverletzungen über deren Internetzugang festgestellt werden.<sup>973</sup> Wie soll sich ein Anschlussinhaber „in angemessener Weise“ davor schützen, dass sein Anschluss nicht für Urheberrechtsverletzungen missbraucht wird? Reicht bereits aus, wenn der drahtlose Internetzugriff mittels WLAN durch eine WPA- oder WPA2-Verschlüsselung gesichert ist? Wie ist die Rechtslage zu beurteilen, falls das als unsicher geltende WEP-Verfahren verwendet oder ein schwaches Passwort benutzt wurde?<sup>974</sup> Eine fortlaufende Überwachung sämtlicher Nutzer eines Internetanschlusses ist für die Anschlussinhaber weder zumutbar noch könnte ein solches Monitoring wirksam umgesetzt werden.<sup>975</sup>

- 419 Da nach geltendem Recht einzig die Staatsanwaltschaft und nur bei Vorliegen eines Tatverdachts die Herausgabe der Identität des Inhabers eines Internetanschlusses verlangen kann, über den mutmasslich eine Straftat im Internet begangen wurde, stellt die vorgeschlagene Erweiterung dieses Auskunftsanspruchs auf die Rechteinhaber zum Zwecke der zivilrechtlichen Verfolgung des Urheberrechtsverstosses eine „Durchbrechung des Fernmeldegeheimnisses im privatrechtlichen Bereich“<sup>976</sup> dar.<sup>977</sup>
- 420 Zwar spricht die AGUR12 davon, dass durch die aufklärenden Hinweise die Möglichkeit geschaffen werden soll, die Nutzer zunächst über die Rechtslage aufzuklären, da eine zu umfassende Rechtsdurchsetzung als problematisch einzustufen sei und als aggressiv empfunden würde.<sup>978</sup> Die geplante Einfüh-

---

<sup>973</sup> AGUR12, Schlussbericht, 75, der Anschlussinhaber soll „nach Erhalt eines aufklärenden Hinweises zur Verhinderung einer zivilrechtlichen Mithaftung im Wiederholungsfall verpflichtet sein, den Weitergebrauch seines Anschlusses für Rechtsverletzungen über *P2P-Netzwerke* in angemessener Weise zu schützen; vgl. auch SOLMECKE/SEBASTIAN/SAHUC, MMR-Aktuell 2011, 316298, welche auf die Problematik hinweisen, dass bei der *Loi HADOPI* nicht nur Täter und Teilnehmer bestraft werden können, sondern gegebenenfalls auch ein Anschlussinhaber, obwohl dieser die Tat nicht begangen hat.

<sup>974</sup> Zur Rechtslage in Deutschland vgl. HOFMANN, ZUM 2014, 658, m.w.H.; HOHLWECK, GRUR 2014, 944 f.

<sup>975</sup> Siehe auch HOFMANN, ZUM 2014, 658 ff.; HOHLWECK, GRUR 2014, 945; GESMANN-NUISSL/WÜNSCHE, GRUR-Int. 2012, 231.

<sup>976</sup> AGUR12, Schlussbericht, 76.

<sup>977</sup> Vgl. Art. 269 StPO sowie Art. 14 f. BÜPF.

<sup>978</sup> AGUR12, Schlussbericht, 75; vgl. auch FREY, ZUM 2014, 556 f. zum sog. Backlash-Effekt bei Massenabmahnungen; zur Problematik von Massenabmahnungen in Deutschland vgl. auch BRÜGGEMANN, MMR 2013, 278 ff.; ADOLPHSEN/MAYER/MÖLLER, NJOZ



rung einer Kausalhaftung der Anschlussinhaber ist aber m.E. als noch wesentlich problematischer und aggressiver einzustufen.<sup>979</sup> In diesem Vorstoss ist der Versuch der Rechteinhaber zu erkennen, sich durch die (verkappte) Einführung einer Kausalhaftung der Anschlussinhaber von dem in der Praxis oft nur schwer zu erbringenden Nachweis zu befreien, welcher Nutzer die Urheberrechtsverletzung begangen hat, falls mehrere Personen gemeinsam einen Internetanschluss nutzen. Die beabsichtigte Verschärfung des Urheberrechts, dass die Anschlussinhaber neu im Wiederholungsfall – nach dem Prinzip „den Letzten beißen die Hunde“ – auch für Urheberrechtsverletzungen Dritter verantwortlich gemacht werden können, ist abzulehnen.<sup>980</sup>

### III. Entfernung urheberrechtsverletzender Inhalte durch *Hosting-Provider* (take down)

#### 1. Vorschlag der AGUR12

Die AGUR12 schlägt in Ziff. 9.3.2. des Schlussberichts vor, dass Hosting- 421  
Provider auf Anzeige der Rechteinhaber oder einer zuständigen Behörde hin unerlaubt hochgeladene Inhalte von ihren *Servern* entfernen müssen.<sup>981</sup> Die

---

2010, 2394 ff.; ferner auch GEIGER, IIC 2011, 469 ff., der eine Pönalisierung der Anschlussinhaber kritisiert.

<sup>979</sup> Daraus kann sich eine Haftung des Anschlussinhabers ergeben, obschon er selbst keine Urheberrechtsverletzung begangen hat.

<sup>980</sup> Die Einführung einer Kausalhaftung im Wiederholungsfall hätte für die Anschlussinhaber zur Folge, dass die Rechteinhaber sowohl den Urheberrechtsverletzer wie auch den Anschlussinhaber auf Schadenersatz verklagen kann (solidarische Haftung, Art. 51 i. V.m. Art. 50 OR). Da bei der Kausalhaftung des Anschlussinhabers nur der Nachweis erbracht werden muss, dass der Anschluss nicht in angemessener Weise gegen Rechtsverletzungen über *P2P-Netzwerke* geschützt wurde, nicht aber, dass der Anschlussinhaber auch tatsächlich die urheberrechtsverletzende Handlung begangen hat, ist zu erwarten, dass die Rechteinhaber ausschliesslich den Anschlussinhaber ins Recht fassen werden. Falls der Anschlussinhaber nicht selbst für die Urheberrechtsverletzung verantwortlich ist, sollte dieser gegen den tatsächlichen Urheberrechtsverletzer wenigstens im Innenverhältnis Regress nehmen können (Art. 51 OR); vgl. auch WULLSCHLEGER, Rz. 367 ff. und Rz. 463, der die Einführung eines Warnhinweismodells ebenfalls ablehnt.

<sup>981</sup> AGUR12, Schlussbericht, 73; WULLSCHLEGER, Rz. 243 ff., der darauf hinweist, dass es keinen Unterschied machen könne, ob der Hinweis von einem Rechteinhaber selbst, einem von diesem ermächtigten Vertreter oder einem Dritten stammt, da es „für die Beurteilung des bewussten Zusammenwirkens des Speicherplatzanbieters an einer Urheber-

Umsetzung soll nach Ansicht der AGUR12 auf dem Wege einer (freiwilligen) Selbstregulierung geschehen, wobei auf den von der Swiss Internet Industry Association (simsa) erlassenen Code of Conduct Hosting (CCH) verwiesen wird.<sup>982</sup>

## 2. Bemerkungen

- 422 Unklarheit besteht zunächst darüber, welche Internetdienste-Anbieter unter den Begriff „*Hosting-Provider*“ zu subsumieren sind. Gemäss Ziff. 2 des CCH ermöglichen Hosting-Dienste den Betreibern von Websites und Applikationen, Inhalte zu speichern, zu verbreiten und Dritten öffentlich zugänglich zu machen. Mit Blick auf die in Ziff. 9.3.3. des Schlussberichts vorgeschlagene Regelung zur Verhinderung des erneuten Hochladens (*stay down*), bei der von *Hosting-Providern* die Rede ist, wird klar, dass hier keine *Webhosting*-Dienste gemeint sind, sondern sog. *Filehoster*.<sup>983</sup> Diese stellen ihren Nutzern online virtuellen Speicherplatz zur Verfügung, auf dem jene unmittelbar und regelmässig auch kostenlos und ohne vorgängige Registrierung digitale Inhalte (Text-, Audio- und Videodateien) abspeichern können.<sup>984</sup>
- 423 An der vorgeschlagenen Mitwirkungspflicht der *Filehoster* ist zu kritisieren, dass diese dazu verpflichtet werden sollen, „unerlaubt hochgeladene Inhalte [zu] entfernen“<sup>985</sup>. Das Hochladen von urheberrechtlich geschützten Werken auf einen virtuellen Speicherplatz im Internet stellt nach schweizerischem Urheberrecht keine urheberrechtswidrige Handlung dar, solange damit nicht gleichzeitig ein unerlaubtes Zugänglichmachen an Dritte verbunden ist.<sup>986</sup> Gestützt auf Art. 19 Abs. 1 lit. a URG dürfen im Rahmen des Privatgebrauchs geschützte Werke kopiert und im Kreis von Personen, die unter sich

---

rechtsverletzung keine Rolle spielt, wer am Werk berechtigt ist“; HOLZNAGEL, GRUR-Int. 2007, 974.

<sup>982</sup> AGUR12, Schlussbericht, 73 f.; FOUNTOLAKIS/FRANCEY, *medialex* 2014, 175; HUG, *medialex* 2014, 56.

<sup>983</sup> Auch *Sharehoster*, *One-Click-Hoster* oder *Cyberlocker* genannt; vgl. auch WULLSCHLEGER, Rz. 239 ff., der von Speicherplatzanbieter spricht.

<sup>984</sup> HUG, *medialex* 2014, 56; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 45 f., zeigt auf, dass die *Hosting-Provider* eine verhältnismässig grosse Distanz zur Mitwirkung aufweisen, da dieser i.d.R. keinen Zugriff auf die einzelnen Inhalte hat; BERANEK ZANON/DE LA CRUZ BÖHRINGER, *sic!* 2013, 665.

<sup>985</sup> AGUR12, Schlussbericht, 73.

<sup>986</sup> So auch WULLSCHLEGER, Rz. 245; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 25 ff.

eng verbunden sind, auch ohne Zustimmung der Rechteinhaber ausgetauscht werden.<sup>987</sup> Ob ein Werk unerlaubt hochgeladen wurde, lässt sich i.d.R. erst nachträglich feststellen, namentlich im Zeitpunkt, da dieses unerlaubt – etwa in einer Linksammlung – öffentlich zugänglich gemacht wurde. Würden *Hosting-Provider* im Rahmen einer Selbstregulierung dazu verpflichtet, sämtliche von den Nutzern hochgeladenen Inhalte nach urheberrechtlich geschützten Werken zu durchsuchen und diese gegebenenfalls zu entfernen, würde dies eine Beschränkung des Privatgebrauchs bedeuten.<sup>988</sup> Die Entfernung hochgeladener Inhalte muss sich deshalb auf solche Werke beschränken, die über einen *Filehoster* unerlaubt i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG zugänglich gemacht werden.<sup>989</sup>

Gemäss dem Vorschlag der AGUR12 soll die Umsetzung der Massnahme 424 auf dem Wege der Selbstregulierung erfolgen.<sup>990</sup> Da die freie oder autonome Selbstregulierung grundsätzlich ohne Mitwirkung des Staates entsteht und auf der Basis freiwilliger Abmachungen beruht, können die einzelnen *Hosting-Provider* nicht zur Teilnahme gezwungen werden. Jedoch löst ein Hinweis<sup>991</sup> aus qualifizierter Quelle, dass urheberrechtlich geschützte Werke – ohne Einwilligung der Rechteinhaber – unerlaubt öffentlich zugänglich gemacht werden, bereits nach geltendem Recht eine Sorgfaltspflicht des

---

<sup>987</sup> Für private Zwecke dürfen urheberrechtlich geschützte Werke vervielfältigt werden, wobei es unerheblich ist, ob die Vervielfältigung auf einem physischen Datenträger beim Nutzer selbst oder auf einem virtuellen Speicherplatz im Internet angefertigt wird; vgl. weiter auch Art. 24 URG betreffend die Zulässigkeit der Herstellung von Sicherungskopien.

<sup>988</sup> Zur Filterung des Datenverkehrs könnte die sog. Deep Packet Inspection (DPI) Filtertechnologie eingesetzt werden, bei der zunächst aus kleinen digitalisierten Fragmenten eines Werks ein „Fingerabdruck“ hergestellt und in einer Datenbank abgelegt wird. Das DPI-System filtert anschliessend die hochgeladenen Inhalte, indem es von diesen ebenfalls „Fingerabdrücke“ erstellt und diese mit der Datenbank vergleicht. Falls eine Übereinstimmung vorliegt, kann die Übertragung gestoppt oder ein Warnhinweis versendet werden; Vgl. dazu MUELLER/KUEHN/SANTOSO, 6.

<sup>989</sup> Etwa indem ein *Download*-Link in einer Linkliste im Internet veröffentlicht wird; WULLSCHLEGER, Rz. 245; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 26, Rz. 55 und Rz. 93.

<sup>990</sup> AGUR12, Schlussbericht, 73 f., „Selbstregulierung [...] im Sinne des von der Swiss Internet Industry Association (simsa) erlassenen „Code of Conduct Hosting“.

<sup>991</sup> WULLSCHLEGER, Rz. 245, wonach die Qualität des Hinweises es dem *Filehoster* ermöglichen muss, die Urheberrechtsverletzung anhand des Hinweises identifizieren zu können. „Zweckdienlich sind beispielsweise der Link bzw. der Dateipfad für die inkriminierte Datei auf dem Rechner eines Speicherplatzanbieters oder auch ein Screenshot“; HOLZNAGEL, GRUR-Int. 2007, 977.

*Filehosters* aus.<sup>992</sup> Bleibt ein *Filehoster* trotz eines solchen Hinweises auf eine Urheberrechtsverletzung untätig, obschon eine Intervention – etwa durch Löschung der entsprechenden Inhalte – für ihn möglich wäre, liegt eine Gehilfenschaft zu einer unerlaubten Zugänglichmachung i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG vor.<sup>993</sup> Die Hilfeleistung der *Filehoster* liegt im aktiven Bereithalten der unerlaubt zugänglich gemachten Werke zum Abruf durch beliebige Dritte. Da Art. 67 Abs. 1 lit. g<sup>bis</sup> URG als Dauerdelikt konzipiert ist, kann der *Filehoster* solange Beihilfe leisten bis das unerlaubt zugänglich gemachte Werk von seinen Servern gelöscht wird.<sup>994</sup> Zudem können die Rechteinhaber gestützt auf Art. 62 Abs. 1 lit. a und lit. b URG vom zuständigen Gericht verlangen, dass dieses eine drohende Verletzung verbietet bzw. eine bestehende Verletzung beseitigt.<sup>995</sup>

## IV. Verhinderung des erneuten Hochladens (*stay down*)

### 1. Vorschlag der AGUR12

- 425 „*Hosting-Provider*, deren Geschäftsmodell offensichtlich auf Rechtsverletzungen durch die Nutzer angelegt ist oder die durch von ihnen zu verantwortende Massnahmen oder Unterlassungen die Gefahr einer rechtsverletzenden

---

<sup>992</sup> WULLSCHLEGER, Rz. 243; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 118, wonach als qualifizierte Quelle Gerichtsurteile, Strafverfolgungsbehörden oder Meldungen von Rechtsinhabern gelten, wobei letzteres umstritten sei; ROSENTHAL, sic! 2006, 514.

<sup>993</sup> WULLSCHLEGER, Rz. 243, spricht von einem bewussten Zusammenwirken mit dem Direktverletzer; HUG, *medialex* 2014, 58, wonach die Hosting Provider dann haften, falls sie „trotz klarem Wissen Rechtsverletzungen nicht unterbinden („*notice and take down*“-Verpflichtung)“; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 155 f., wonach „erst die konkrete Kenntnisnahme, gepaart mit der beharrlichen Weigerung des Filehosters, die Dateien zu entfernen und ein beachtlicher Zeitlauf seit der Notice“ eine Strafbarkeit auszulösen vermag; ROSENTHAL, sic! 2006, 512, der sich u.a. mit der Frage beschäftigt, ob eine Unterlassung durch Nichtverhindern des Unrechts eines Dritten vorliegt oder eine Gehilfenschaft durch aktives Fördern des Haupttäters.

<sup>994</sup> S.o. Rz. 130; a.A. BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 156 ff.

<sup>995</sup> Vgl. auch WULLSCHLEGER, Rz. 259 ff., mit weiteren Hinweisen zum Unterlassungs- und Beseitigungsanspruch; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 57 ff.; ROSENTHAL, sic! 2006, 512 ff., m.w.H. zur zivilrechtlichen Haftung von Internet-Providern für das Unrecht Dritter.

Nutzung absichtlich fördern, sollen auf Anzeige des Rechteinhabers hin unerlaubt hochgeladene Inhalte entfernen und zusätzlich das erneute unerlaubte Hochladen solcher Inhalte im Rahmen des Zumutbaren verhindern<sup>996</sup>. Die AGUR12 hält in ihrem Schlussbericht fest, dass solche Fälle nicht durch eine Selbstregulierung erfasst werden könnten, weshalb die erforderlichen gesetzlichen Grundlagen zu schaffen seien.

## 2. Bemerkungen

Zunächst können gegen diesen Vorschlag der AGUR12 die gleichen Einwände vorgebracht werden wie schon beim Vorschlag zur Entfernung unerlaubt hochgeladener Inhalte (*take down*).<sup>997</sup> Das (erneute) Hochladen geschützter Werke auf die *Server* eines Online-Speicherdienstes stellt bei isolierter Betrachtung keine urheberrechtsverletzende Handlung dar. Ein Verstoss gegen das Urheberrecht liegt erst dann vor, wenn das geschützte Werk im Anschluss an den *Upload* auf den virtuellen Speicherplatz ohne die Einwilligung der Rechteinhaber unerlaubt i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG zugänglich gemacht wird.<sup>998</sup>

Gemäss Vorschlag der AGUR12 soll gewissen *Filehostern*, deren Geschäftsmodell offensichtlich auf Rechtsverletzungen durch die Nutzer angelegt ist, neben der Pflicht zur Durchführung reaktiver Massnahmen (*take down*) kumulativ eine Verpflichtung zur Vornahme proaktiver Massnahmen zur Verhinderung zukünftiger Urheberrechtsverletzungen (*stay down*) auferlegt werden.<sup>999</sup> Die Forderung an die *Filehoster*, das wiederholte Hochladen von geschützten Werken zu verhindern ist in verschiedener Hinsicht zu beanstanden. Zunächst können die *Filehoster* nicht unterbinden, dass eine gelöschte Datei erneut hochgeladen wird.<sup>1000</sup> Weiter liegt erst dann eine Urheberrechtsverletzung vor, wenn der *Link* zur erneut hochgeladenen Datei un-

---

<sup>996</sup> AGUR12, Schlussbericht, 74.

<sup>997</sup> S.o. Rz. 423.

<sup>998</sup> Siehe auch WULLSCHLEGER, Rz. 245; BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 25.

<sup>999</sup> Der Vorschlag der AGUR12 ist stark auslegungsbedürftig formuliert. Ob ein auf Urheberrechtsverletzungen angelegtes Geschäftsmodell vorliegt, wird letztlich durch ein Gericht anhand der konkreten Sachlage im Einzelfall zu beurteilen sein.

<sup>1000</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 64; wonach die *Filesharer* die Datei etwa mit einem neuen Titel versehen bzw. anderweitig bearbeiten können.

erlaubt öffentlich zugänglich gemacht wird.<sup>1001</sup> Deshalb darf der *Filehoster* nur solche geschützten Werke von seinen *Servern* löschen, die nachweislich unerlaubt zugänglich gemacht worden sind.<sup>1002</sup> Ansonsten liegt eine unerlaubte Löschung an den hochgeladenen Inhalten vor.<sup>1003</sup> Sodann können die *Filehoster* nicht verhindern, dass eine erneut hochgeladene Datei über einen *Remote-Server* mit dem alten *Link* verknüpft wird und so weiterhin über den alten *Link* heruntergeladen werden kann.<sup>1004</sup> Schliesslich können die *Filehoster* selbst keine *Links* löschen und selbst mit dem Einsatz von *Webcrawlern* können nur jene *Links* überprüft werden, die öffentlich zugänglich sind.<sup>1005</sup> Mangels Umsetzbarkeit und Verhältnismässigkeit ist die Einführung einer umfassenden Kontrollpflicht zur Verhinderung zukünftiger Rechtsverletzungen für die *Filehoster* abzulehnen.<sup>1006</sup>

- 428 Alternativ könnte darüber nachgedacht werden, die *Filesharing*-Funktionen bei Online-Speicherdiensten auf ein Mass zu beschränken, welches mit dem Privatgebrauch nach Art. 19 Abs. 1 lit. a URG in Einklang steht. Zwar sieht das Schweizer Urheberrechtsgesetz keine mengenmässige Begrenzung der zum Privatgebrauch erlaubten Kopien vor – „doch ergibt sich eine solche aus dem privaten Zweck und dem Erfordernis der engen Verbundenheit“<sup>1007</sup>.

---

<sup>1001</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 64, weist zutreffend darauf hin, dass i.d.R. im Zeitpunkt der Veröffentlichung des *Links* „die *Verletzung bereits begangen* [ist], sie kann damit nicht mehr verhindert werden“.

<sup>1002</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 113.

<sup>1003</sup> Vgl. aber AGUR12, Schlussbericht, 76, wonach für die *Access*- und *Hosting-Provider* „Haftungsfreistellungsbestimmungen ausdrücklich gesetzlich vorzusehen [sind]“. Einer solchen Haftungsbefreiung stehen legitime Interessen der betroffenen Nutzer gegenüber, rechtlich gegen einen *Hosting-Provider* vorgehen zu können, wenn diese etwa hochgeladene Inhalte zu Unrecht von deren *Server* entfernen. Die vorgeschlagene Haftungsbefreiung könnte die *Hosting-Provider* auch dazu verleiten, gespeicherte Inhalte sorgfaltpflichtwidrig zu extensiv zu löschen, falls rechtliche Konsequenzen seitens der betroffenen Nutzer von vornherein ausgeschlossen sind.

<sup>1004</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 65 und Rz. 114.

<sup>1005</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 65 und Rz. 114, sobald die *Links* innerhalb einer sog. *Closed User-Gruppe* aufgelistet werden, können diese nicht überprüft werden.

<sup>1006</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 116; ROSENTHAL, sic! 2006, 513; siehe auch ROHN, 204 ff., der bei *Hosting-Providern* eine präventive Kontrollpflicht für den zivilrechtlichen Bereich ablehnt.

<sup>1007</sup> GASSER, SHK URG, Art. 19 N 9b; ebenso REHBINDER/VIGANÒ, Art. 19 N 18; a.A. BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 29, die gegen eine Beschränkung der *Downloads* auf eine bestimmte Anzahl einwendet, dass hierdurch auch legale Nutzungen verunmöglicht werden.

Durch die Implementierung eines Content-ID-Systems kann erreicht werden, dass die Beschränkungen nur dann greifen, wenn es sich bei den hochgeladenen Inhalten um urheberrechtlich geschützte Werke handelt (urheberrechtsfreie Dateien könnten weiterhin unlimitiert geteilt werden).<sup>1008</sup> Die maximale Anzahl möglicher *Downloads* oder gleichzeitiger Streams muss sodann so gewählt werden, dass diese mit dem Privatgebrauch korrespondiert.<sup>1009</sup> Ziel der Beschränkung ist gerade nicht eine Beschränkung des erlaubten Privatgebrauchs, sondern die Verhinderung von massenhaften Urheberrechtsverletzungen bei Online-Speicherdiensten durch eine unbegrenzte Anzahl *Downloads* und Streams von der gleichen Quelle.

## V. Zugangssperren durch *Access-Provider*

### 1. Vorschlag der AGUR12

In „schwerwiegenden Fällen“ sollen in der Schweiz befindliche Access-  
Provider<sup>1010</sup> auf behördliche Anweisung hin den Zugang zu Portalen, auf  
denen Inhalte aus „offensichtlich illegalen Quellen“ angeboten werden, über  
IP- und DNS<sup>1011</sup>-Blocking sperren. Im Gegenzug sollen die Provider für die  
Aufwände, die ihnen durch die Errichtung von Zugangssperren entstehen,  
angemessen entschädigt werden. Die AGUR12 verzichtet auf eine nähere  
Umschreibung, wann ein schwerwiegender Fall vorliegt und begnügt sich  
stattdessen mit dem Hinweis, dass bei der Sperrung illegaler Inhalte die Mit-  
sperrung legaler Angebote (*Overblocking*) so weit als möglich zu vermeiden  
sei. Zudem dürfe durch die Internetsperren die technische Funktionsfähigkeit  
des IP- und DNS-Systems nicht gefährdet werden. Die zur Umsetzung erforder-

<sup>1008</sup> REHBINDER, ZUM 2013, 248 ff., m.w.H.; *YouTube* verwendet ein System namens *Content ID* welches die hochgeladenen Inhalte prüft und mit einer Datenbank abgleicht, die von den Rechteinhabern an *YouTube* übermittelt wurden. Falls die hochgeladenen Inhalte mit einem ihrer Werke übereinstimmt, können die Rechteinhaber darüber entscheiden, was mit dem Video (im jeweiligen Land) geschieht; siehe <<https://www.youtube.com/yt/copyright/de>> (besucht 25. August 2015).

<sup>1009</sup> Z.B. eine Limitierung je hochgeladene Datei auf 20 *Downloads* pro Tag bzw. 50 *Downloads* pro Monat sowie eine Beschränkung auf maximal zehn simultane Stream-Abrufe.

<sup>1010</sup> Z.B. Swisscom, Sunrise, UPC Cablecom oder green.ch; GREVE, 116 f., m.w.H.

<sup>1011</sup> Weiterführend dazu SCHREINER, 90 ff. und TANENBAUM/ WETHERALL, 703 ff.

derlichen Gesetzesgrundlagen seien zu schaffen und die Einhaltung der Rechtsweggarantie zu beachten.<sup>1012</sup>

## 2. Technische Grundlagen

### A. DNS-Sperren

#### a) Funktionsweise

430 Der Abruf einer Webseite gestaltet sich i.d.R. so, dass der Nutzer den *Domainnamen*<sup>1013</sup> in die *Browserzeile* eingibt und sodann eine Anfrage an einen *DNS-Server* seines *Access-Providers* sendet.<sup>1014</sup> Der *DNS-Server* ermittelt die hinter jeder *Domain* stehende numerische *IP-Adresse*<sup>1015</sup> und leitet die Anfrage an den *Server* mit der dazugehörigen *IP-Adresse* weiter.<sup>1016</sup> Bei *DNS-Sperren* wird die Zuordnung von *Domainname* und *IP-Adresse* auf dem *DNS-Server* des *Access-Providers* geändert oder gelöscht, mit dem Resultat, dass die Übersetzung und die daran anschließende Weiterleitung zur Ziel-*IP-Adresse* unterbunden wird.<sup>1017</sup> Alternativ kann der Router so konfiguriert werden, dass die Nutzer nicht die gewünschte Webseite aufrufen können und stattdessen auf eine andere Webseite umgeleitet werden.<sup>1018</sup> Aus datenschutzrechtlicher Perspektive sind *DNS-Sperren* unproblematisch, da keine personenbezogenen Daten – wie etwa die *IP-Adresse* des die Anfrage tätigen Nutzers – erhoben werden.<sup>1019</sup>

---

<sup>1012</sup> Zum Ganzen AGUR12, Schlussbericht, 74.

<sup>1013</sup> Z.B. kinox.to.

<sup>1014</sup> LEISTNER/GRISSE, GRUR 2015, 22.

<sup>1015</sup> Z.B. 91.202.61.170 (kinox.to), *IP-Adresse* abrufbar unter <<http://ipaddress.com/ip-lookup>> (besucht 25. August 2015).

<sup>1016</sup> LEISTNER/GRISSE, GRUR 2015, 22; BALTISSER, 7; TANENBAUM/WETHERALL, 703 ff.; SCHWARZENEGGER, Sperrverfügungen, 275 f.; STADLER, MMR 2002, 345.

<sup>1017</sup> LEISTNER/GRISSE, GRUR 2015, 22; GREVE, 125 f.; HENNEMANN, 231; DURNER, ZUM 2010, 833; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 14 ff.

<sup>1018</sup> NAZARI-KHANACHAYI, GRUR 2015, 117, verwendet hierfür den Begriff „DNS-basierte-Umleitung“; LEISTNER/GRISSE, GRUR 2015, 22, weisen darauf hin, dass die DNS-Sperre zwar den Zugang zur betroffenen *Domain* vollständig blockiert, diese aber in deren Existenz nicht tangiert, weshalb verschiedene Umgehungsmöglichkeiten bestehen bleiben; GREVE, 126 ff., zeigt auf, dass es auch bei der Umsetzung von DNS-Sperren zu einem *Overblocking* kommen kann; FREY/RUDOLPH/OSTER, MMR-Beil. 2012, 2; STADLER, MMR 2002, 345.

<sup>1019</sup> Vgl. LEISTNER/GRISSE, GRUR 2015, 23; KROPP, 164, 174; DURNER, ZUM 2010, 845.



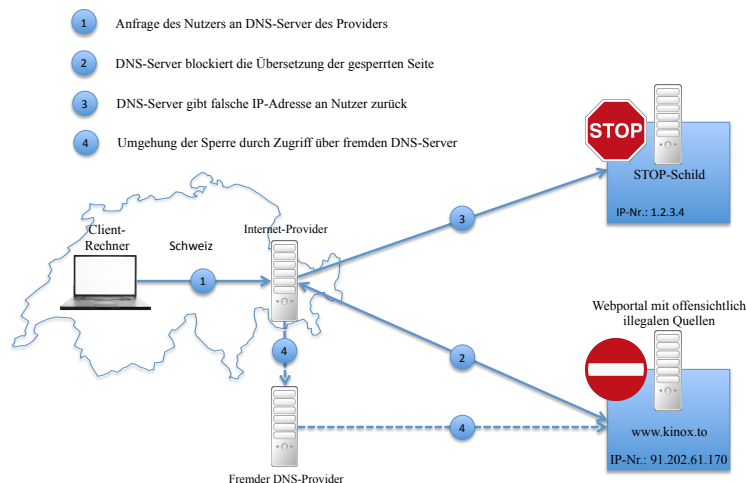


Abbildung 15: DNS-Sperren, Quelle: <<http://www.privacyfoundation.ch/de/service/dns-sperren.html>> (besucht 3.7.2015)

## b) Umgehungsmöglichkeiten

Die *DNS-Sperren* lassen sich leicht umgehen, indem die numerische *IP-Adresse* direkt in den *Browser* eingegeben wird.<sup>1020</sup> Alternativ dazu kann eine *DNS-Sperre* auch durch den gezielten Zugriff auf andere *DNS-Server*<sup>1021</sup>, welche die Weiterleitung der Anfrage nicht unterbinden, umgangen werden.<sup>1022</sup> Um solche „trivialen Umgehungsmassnahmen einer DNS-Sperre“ zu verhindern schlagen PFITZMANN/KÖPSELL/KRIEGELSTEIN deshalb vor, dass die *Access-Provider* kumulativ Sperren einsetzen, die basierend auf Kriterien der Transport- bzw. Anwendungsschicht verhindern, dass ein Nutzer alternative *DNS-Server* verwenden kann bzw. an die benötigten *DNS-Informationen* gelangt.<sup>1023</sup> Als weitere Möglichkeit zur Umgehung von

<sup>1020</sup> LEISTNER/GRISSE, GRUR 2015, 22; GREVE, 126 f.; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 52; SCHWARZENEGGER, Sperrverfügungen, 276; STADLER, MMR 2002, 345.

<sup>1021</sup> Z.B. Google Public DNS, <<https://developers.google.com/speed/public-dns/docs/using>> (besucht 25. August 2015).

<sup>1022</sup> LEISTNER/GRISSE, GRUR 2015, 22; FRECH, Fn. 1356, m.w.H.; ZINN, digma 2008, 115 f.; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 53, m.w.H.

<sup>1023</sup> PFITZMANN/KÖPSELL/KRIEGELSTEIN, 53 i.V.m. 37 f.; ablehnend LEISTNER/GRISSE, GRUR 2015, 22, mit dem Hinweis, dass „eine komplette Sperrung des Ports 54, über den DNS-Anfragen standardmässig laufen, zur Verhinderung des Zugriffs auf andere Name-Server [...] als zu weitreichender Eingriff in den gesamten Internetverkehr abzulehnen [ist]“.

*DNS-Sperren* kann der Nutzer seine Internetkommunikation über einen *Proxy-Server* umleiten lassen, der typischerweise einen anderen *DNS-Server* verwendet.<sup>1024</sup>

## **B. IP-Sperren**

### **a) Funktionsweise**

- 432 Bei der Internetkommunikation werden über das *IP-Protokoll* Datenpakete via Router versendet.<sup>1025</sup> Die Kopfzeile (*Header*) beinhaltet insbesondere die *Ziel-IP-Adresse* und die *Quell-IP-Adresse*. Sog. *Routingtabellen* sorgen dafür, dass die Datenpakete „von Router zu Router bis an ihr Ziel“<sup>1026</sup> weitergeleitet werden.<sup>1027</sup> Mit *IP-Sperren* kann der Zugriff auf bestimmte Webseiten verhindert werden, indem entsprechende *IP-Adressen* aus der Routingtabelle entfernt bzw. durch bestimmte Vergleichsregeln ergänzt werden.<sup>1028</sup> Die Vergleichsregel schlägt an, sobald ein Datenpaket im *Header* als *Ziel-IP-Adresse* eine der gesperrten *IP-Adressen* enthält und löst einen „discard“-Befehl aus, der dazu führt, dass das betroffene Datenpaket verworfen wird.<sup>1029</sup> Da bei *IP-Sperren* auch sämtliche hinter einer *IP-Adresse* liegenden *URL* (*Uniform Resource Locator*) mitgesperrt werden, ist hier die Gefahr eines *Overblocking* gross.<sup>1030</sup> Soweit die *Access-Provider* keine über den

---

<sup>1024</sup> SPINDLER, GRUR 2014, 831; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 53

<sup>1025</sup> GREVE, 123.

<sup>1026</sup> LEISTNER/GRISSE, GRUR 2015, 23.

<sup>1027</sup> NAZARI-KHANACHAYI, GRUR 2015, 117; LEISTNER/GRISSE, GRUR 2015, 23; SCHREINER, 84.

<sup>1028</sup> NAZARI-KHANACHAYI, GRUR 2015, 117, spricht diesbezüglich von einer „Router-basierten IP-Adressenausschluss“; LEISTNER/GRISSE, GRUR 2015, 23; SCHREINER, 84; DURNER, ZUM 2010, 833.

<sup>1029</sup> LEISTNER/GRISSE, GRUR 2015, 23; GREVE, 123 f.; TANENBAUM/WETHERALL, 531; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 15; SCHWARZENEGGER, Sperrverfügungen, 274.

<sup>1030</sup> Ein *Overblocking* liegt vor, wenn durch die Sperrmassnahme nebst illegalen Angeboten auch legale Angebote mitgesperrt werden; LEISTNER/GRISSE, GRUR 2015, 24, verweisen auf Fälle des „Virtual Hostings“, bei dem sämtliche unter einer *IP-Adresse* gehosteten Websites von der Sperre betroffen sind; WULLSCHLEGER, Rz. 453, zweifelt deshalb an, dass eine *IP-Adressblockade* umgesetzt werden kann, ohne dabei die „technische Funktionsfähigkeit des IP- oder DNS-Systems“ zu gefährden; ANGELOPOULOS, GRUR-Int. 2014, 1092; GREVE, 124, 133, wendet gegen *IP-Sperren* ein, dass diese „grundsätzlich zu immensen Kollateralschäden [führen], da eine hinreichende Zielgenauigkeit oftmals nicht gewährleistet ist und daher eine grosse Anzahl neutraler Inhalte beeinträchtigt zu werden droht“; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 55; SCHWARZENEGGER, Sperrverfügungen, 275.

Verbindungsaufbau hinausgehenden Daten erheben oder weitergehend verwenden, sind auch *IP-Sperren* datenschutzrechtlich unbedenklich.<sup>1031</sup>

### **b) Umgehungsmöglichkeiten**

Auf Transportebene können auch *IP-Sperren* relativ einfach umgangen werden, indem offene *Proxy-Server*, *Anonymisierungs-Dienste*<sup>1032</sup> oder virtuelle private Netzwerke (*VPN*) eingesetzt werden.<sup>1033</sup> Die Betreiber der gesperrten Webseite können die *IP-Sperre* umgehen, indem sie ihre Internetpräsenz auf eine andere *IP-Adresse* verlegen.<sup>1034</sup>

## **3. Bemerkungen**

### **A. Zuständigkeit**

Bisher sperrten in der Schweiz viele *Access-Provider* – aufgrund einer Liste der KOBK<sup>1035</sup> – freiwillig den Zugang zu gewissen Webseiten mit mutmasslich kinderpornografischen Inhalten.<sup>1036</sup> In Einzelfällen wurde der Zugang auch aufgrund gerichtlich angeordneter Netzsperrungen blockiert.<sup>1037</sup> Gemäss dem Vorschlag der AGUR12 soll die KOBK selbst oder eine entsprechende neue Behördenstelle dazu ermächtigt werden, durch Anweisung an die in der Schweiz befindlichen *Access-Provider* den Zugang zu „Webportalen mit offensichtlich illegalen Quellen“ mittels *IP-* und *DNS-Blocking* sperren zu

<sup>1031</sup> Vgl. zum deutschen Recht LEISTNER/GRISSE, GRUR 2015, 24; DURNER, ZUM 2010, 845; a.A. KROPP, 164 f.

<sup>1032</sup> z.B. *TOR* oder *JonDo*; vgl. auch WULLSCHLEGER, Rz. 32, m.w.H.

<sup>1033</sup> WULLSCHLEGER, Rz. 43, zeigt auf, dass die Anonymisierungs- oder Proxymbieter den Nutzern bloss einen derivativen Zugang zum Internet ermöglichen, weshalb diese auch nicht zur Speicherung von Verkehrsdaten verpflichtet sind; LEISTNER/GRISSE, GRUR 2015, 24; THIESEN, MMR 2014, 805, m.H. zu den technischen Möglichkeiten und Schwierigkeiten der Implementierung von Filtertechniken bei Anonymisierungsdiensten; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 52 f. und 65; SCHWARZENEGGER, Sperrverfügungen, 275.

<sup>1034</sup> LEISTNER/GRISSE, GRUR 2015, 24; GREVE, 124; PFITZMANN/KÖPSELL/KRIEGELSTEIN, 55; SCHWARZENEGGER, Sperrverfügungen, 275, erwähnt zudem die Möglichkeit der Spiegelung der Inhalte auf andere *Webserver* (*Mirroring*).

<sup>1035</sup> Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität.

<sup>1036</sup> WULLSCHLEGER, Rz. 449; SECO, Roundtable zum Urheberrecht, 8; ZINN, digma 2008, 116.

<sup>1037</sup> FOUNTOULAKIS/FRANCEY, medialex 2014, 181, m.w.H.; Urteil 1B.242/2009 des Bundesgerichts vom 21. Oktober 2009, Erw. 2.

lassen. Der Entscheid über den Erlass einer Netzsperrung würde so einer vorgängigen richterlichen Prüfung entzogen.

## **B. Vereinbarkeit von Zugangssperren mit den Grundrechten der Betroffenen**

- <sup>435</sup> Gestützt auf Art. 16 Abs. 3 BV hat jede Person das Recht, Informationen frei zu empfangen, aus allgemein zugänglichen Quellen zu beschaffen und zu verbreiten.<sup>1038</sup> Durch die Sperrung des Zugangs zu frei zugänglichen Webseiten<sup>1039</sup> mittels *IP*- und *DNS-Blocking* werden sowohl die Meinungs- und Informationsfreiheit (Art. 16 BV) als auch die Medienfreiheit (Art. 17 BV) tangiert.<sup>1040</sup> Die Zugangssperre stellt aus Sicht der Betreiber der Webseite einen Eingriff in deren Wirtschaftsfreiheit (Art. 27 BV) dar. Schliesslich kann auch die in Art. 26 BV verankerte Eigentumsgarantie verletzt sein – etwa wenn der Zugang zu einem *Filehosting-Dienst* gesperrt wird und ein Nutzer so den Zugang zu seinen Daten verliert. Die mit der Zugangssperre verbundenen Eingriffe in die Grundrechte der Beteiligten sind deshalb nur dann zulässig, wenn die einzelnen in Art. 36 BV aufgeführten Voraussetzungen für die Einschränkung von Grundrechten, kumulativ erfüllt sind.<sup>1041</sup>

### **a) Genügende gesetzliche Grundlage**

- <sup>436</sup> Die AGUR12 hält in ihrem Schlussbericht fest, dass die erforderlichen gesetzlichen Grundlagen zu schaffen und die Rechtsweggarantie zu beachten seien. Da Zugangssperren als schwerwiegende Einschränkungen zu qualifizieren sind, ist eine Grundlage in einem formellen Gesetz erforderlich. Dies könnte durch Aufnahme eines neuen Art. 69b URG geschehen. Darin müsste einerseits die Kompetenz der Behörde zur Anordnung von *DNS*- und *IP-Sperren* sowie die Mitwirkungspflicht der *Access-Provider* bei der Einrichtung der Zugangssperren geregelt werden. Damit die Rechtsweggarantie gewahrt bleibt, muss es den Betroffenen möglich sein, gegen die angeordnete Sperrverfügung ein Rechtsmittel einzulegen.

---

<sup>1038</sup> BGE 137 I 16, Erw. 2.2.

<sup>1039</sup> Z.B. einem *Streaming-Portal*, einem *Filehosting-Dienst* oder einer Webseite, auf der u.a. Links zum *Downloaden* von geschützten Werken angeboten werden.

<sup>1040</sup> LEUENBERGER, sic! 2014, 726; SCHWARZENEGGER, Sperrverfügungen, 266.

<sup>1041</sup> SCHWEIZER, Art. 36 N 22.

**b) Öffentliches Interesse oder Schutz von Grundrechten Dritter**

Ferner muss die Einschränkung von Grundrechten durch ein öffentliches Interesse oder den Schutz von Grundrechten Dritter gerechtfertigt sein.<sup>1042</sup> Als öffentliches Interesse kommt vorliegend ein Interesse der Öffentlichkeit an einer wirksamen Durchsetzung des Urheberrechts in Betracht.

**c) Verhältnismässigkeit**

Der Grundsatz der Verhältnismässigkeit ist nach bundesgerichtlicher Rechtsprechung gewahrt, wenn die „behördliche Massnahme für das Erreichen des im öffentlichen (oder privaten) Interesse liegenden Zieles geeignet und erforderlich ist und sich für die Betroffenen in Anbetracht der Schwere der Grundrechtseinschränkung [als] zumutbar und verhältnismässig erweist“<sup>1043</sup>.

**aa) Eignung**

Eine staatliche Massnahme ist geeignet, wenn durch sie das öffentliche Interesse auch tatsächlich wahrgenommen werden kann.<sup>1044</sup> Wie zuvor aufgezeigt wurde, lassen sich *DNS-* und *IP-Sperren* mit relativ geringem Aufwand umgehen.<sup>1045</sup> Werden die beiden Sperrmassnahmen miteinander kombiniert, können aber zumindest besonders triviale Umgehungsmassnahmen effektiver verhindert werden.<sup>1046</sup> Obschon auch bei Verknüpfung verschiedener Sperrtechniken weiterhin Möglichkeiten zur Umgehung bestehen, sind diese dennoch grundsätzlich geeignet, Urheberrechtsverstösse zu verhindern bzw. zu erschweren.<sup>1047</sup>

---

<sup>1042</sup> BGE 138 II 173, Erw. 7.1.

<sup>1043</sup> BIAGGINI, Art. 36 N 23; BGE 132 I 49, Erw. 7.2.; BGE 126 I 112, Erw. 5 b).

<sup>1044</sup> SCHWEIZER, Art. 36 N 23.

<sup>1045</sup> NAZARI-KHANACHAYI, GRUR 2015, 117; LEISTNER/GRISSE, GRUR 2015, 22, 24; HEID, 123; PFITZMANN/KÖPSELL/KRIEGLSTEIN, 65; SCHWARZENEGGER, Sperrverfügungen, 275 f.

<sup>1046</sup> LEISTNER/GRISSE, GRUR 2015, 26 f., die aber eine Kombination aus *IP-* und *URL-Sperren* favorisieren; PFITZMANN/KÖPSELL/KRIEGLSTEIN, 55.

<sup>1047</sup> LEISTNER/GRISSE, GRUR 2015, 110 f.; NORDEMANN, ZUM 2014, 500; a.A. WULLSCHLEGER, Rz. 453 ff. und Rz. 466, hält das Sperren von Webseiten für kein geeignetes Mittel um den Zugang zu unerlaubt zugänglich gemachten Werken, wirksam verhindern zu können.

*bb) Erforderlichkeit*

- 440 „Der Eingriff darf in sachlicher, räumlicher, zeitlicher und personeller Hinsicht nicht einschneidender sein als notwendig“<sup>1048</sup>. Eine Massnahme hat zu unterbleiben, falls eine andere, gleich geeignete aber mildere Massnahme für den verfolgten Zweck ausreichen würde.<sup>1049</sup> Vorliegend könnte das Ziel allenfalls auch durch eine *URL-Sperre* erreicht werden: Dadurch kann der Zugriff auf einzelne Webseiten eines Internetauftritts zielgenau gesperrt werden.<sup>1050</sup> Die Gefahr eines *Overblocking* wird so reduziert.<sup>1051</sup>

*cc) Verhältnismässigkeit im engeren Sinn (Zumutbarkeit)*

- 441 Zwischen dem mit dem Eingriff gesteckten Ziel und der zu seiner Erreichung notwendigen Grundrechtsbeschränkung muss ein vernünftiges Verhältnis bestehen.<sup>1052</sup> Eine Massnahme ist unverhältnismässig und hat zu unterbleiben, wenn in einem konkreten Fall die negativen Auswirkungen schwerer wiegen als das öffentliche Interesse an deren Vornahme.<sup>1053</sup>
- 442 Die Sperrung einer Internetseite stellt einen erheblichen Eingriff in die Informationsfreiheit der Nutzer dar, weshalb Netzsperrungen nur sehr restriktiv und einzig in schweren Fällen eingesetzt werden sollten. Beim Einsatz von *DNS-* und *IP-Sperren* sind im Rahmen der Prüfung der Zumutbarkeit insbesondere die negativen Auswirkungen eines *Overblocking* zu berücksichtigen. Besonders problematisch ist eine Zugangssperre zu einer gesamten Webseite mittels *DNS-* und *IP-Blocking*, wenn auf einer Webseite nebst illegalen Inhalten auch legale Inhalte angeboten werden.<sup>1054</sup>

---

<sup>1048</sup> BGE 126 I 112, Erw. 5b); BGE 124 I 40, Erw. 3e; 118 Ia 427, Erw. 7a.

<sup>1049</sup> BGE 133 I 77, Erw. 4.1; BGE 132 I 49, Erw. 7.2; BGE 126 I 112, Erw. 5b.

<sup>1050</sup> LEISTNER/GRISSE, GRUR 2015, 25 f.; ablehnend HEID, 123, die darauf hinweist, dass die Einrichtung eines URL-Filters mit immensem Aufwand verbunden wäre.

<sup>1051</sup> LEISTNER/GRISSE, GRUR 2015, 24; ANGELOPOULOS, GRUR-Int. 2014, 1092; PFITZMANN/KÖPSELL/KRIEGLSTEIN, 54 f.; SCHWARZENEGGER, Sperrverfügungen, 275 f.

<sup>1052</sup> BIAGGINI, Art. 36 N 23; SCHWARZENEGGER, Sperrverfügungen, 279.

<sup>1053</sup> HÄFELIN/HALLER/KELLER, Rz. 320 ff.

<sup>1054</sup> WULLSCHLEGER, Rz. 454, der DNS- oder IP-Sperren für keine geeigneten Mittel zur Bekämpfung von Urheberrechtsverletzungen hält und auf die Gefahr eines *Overblocking* verweist. Zudem wird bemängelt, dass die Sperren die fraglichen Inhalte nicht beseitigen, sondern bloss deren Verfügbarkeit erschweren; METZGER, GRUR 2012, 384 f., plädiert dafür, dass beim Einsatz technischer Massnahmen die nicht hinreichend zwischen erlaubten und unerlaubten Inhalten unterscheiden, der Schutz des geistigen Eigentums hinter das Interesse am freien Zugang zu Informationen zurücktreten muss.

## Zusammenfassung wesentlicher Ergebnisse

### I. Streaming aus der Perspektive der Anbieter

Das Anbieten urheberrechtlich geschützter Werke auf dem Wege des nicht- 443  
linearen On-Demand-Streaming oder linearen Near-on-Demand-Streaming  
setzt ein vorgängiges Hochladen und Abspeichern des Werks auf einen Web-  
oder Streaming-Server voraus, weshalb das in Art. 10 Abs. 2 lit. a URG sta-  
tuierte Vervielfältigungsrecht tangiert ist.<sup>1055</sup> Da beim linearen Live-  
Streaming ebenfalls technisch bedingte transitorische Vervielfältigungen auf  
dem Server des Anbieters hergestellt werden, ist auch hier das Vorliegen  
einer urheberrechtlich relevanten Vervielfältigung i.S.v. Art. 10 Abs. 2 lit. a  
URG zu bejahen.<sup>1056</sup>

Das Bereithalten eines Werks zum Abruf über das Internet, mittels On- 444  
Demand-Streaming ist als öffentliche Zugänglichmachung i.S.v. Art. 10  
Abs. 2 lit. c URG zu qualifizieren.<sup>1057</sup> Im Unterschied dazu liegt beim Live-  
Streaming sowie beim Near-On-Demand-Streaming keine Zugänglichma-  
chung nach Art. 10 Abs. 2 lit. c URG vor, weil nicht der Rezipient, sondern  
der Anbieter über den Zeitpunkt der Werkwiedergabe entscheidet.<sup>1058</sup> Folg-  
lich sind das lineare Live-Streaming und das Near-On-Demand-Streaming  
unter das Senderecht nach Art. 10 Abs. 2 lit. d URG zu subsumieren.<sup>1059</sup>  
Falls ein geschütztes Werk, das über Radio, Fernsehen oder ähnliche Verfah-  
ren gesendet wird, zeitgleich mittels Live-Streaming ins Internet gestellt  
wird, ist das Weitersenderecht nach Art. 10 Abs. 2 lit. e URG tangiert.<sup>1060</sup>

Im Regelfall liegt beim Streaming kein Eingriff in die Werkintegrität nach 445  
Art. 11 URG vor, da sich die Änderung auf rein technische Umwandlungen  
des Werks beschränkt. Ein Eingriff in die Werkintegrität ist etwa denkbar,  
wenn eine Bannerwerbung in das Wiedergabefenster des Players eingebun-  
den wird oder falls Werbebotschaften eingeblendet werden.<sup>1061</sup>

---

<sup>1055</sup> S.o. Rz. 46 ff.

<sup>1056</sup> S.o. Rz. 48 ff.

<sup>1057</sup> S.o. Rz. 53.

<sup>1058</sup> S.o. Rz. 54.

<sup>1059</sup> S.o. Rz. 57.

<sup>1060</sup> S.o. Rz. 149 f.

<sup>1061</sup> Vgl. dazu Rz. 58.

- 446 Normalerweise erhält der Nutzer beim Streaming keinen dauerhaften Zugriff auf das Werkexemplar. Die technisch bedingten Vervielfältigungen, welche bei der Werkwiedergabe mittels Streaming-Verfahren auf dem Nutzerrechner anfallen, sind vielmehr lediglich vorübergehender Natur. Zudem ist auf das dem Streaming zugrunde liegende Vertragsverhältnis zwischen den Rechteinhabern und dem Nutzer nicht das Kaufvertragsrecht, sondern das Mietrecht oder die Gebrauchsleihe analog anwendbar. Folglich ist der in Art. 12 URG statuierte Erschöpfungsgrundsatz beim Streaming von urheberrechtlich geschützten Werken nicht tangiert, da die hierzu erforderliche Veräusserungshandlung fehlt.<sup>1062</sup>
- 447 Mittels *Inline-Framing* können Multimediainhalte auf einer fremden Webseite eingebettet und dort wiedergegeben werden, obwohl sich die Dateien auf einer anderen Webseite befinden, mithin auf einem anderen Server abgelegt sind.<sup>1063</sup> Da beim *Framing* keine Vervielfältigung des Werks auf den *Servern* des verweisenden Betreibers stattfindet, ist das Vervielfältigungsrecht nach Art. 10 Abs. 2 lit. a URG nicht berührt. Komplizierter gestaltet sich die Beantwortung der Frage, ob beim *Framing* ein Zugänglichmachen i.S.v. Art. 10 Abs. 2 lit. c URG vorliegt. Das Vorliegen einer öffentlichen Zugänglichmachung sollte erst dann bejaht werden, wenn die geschützten Werke durch den Einsatz von *Links* oder *Frames*, einem neuen Publikum zugänglich gemacht werden. Dabei soll das Vorliegen eines neuen Publikums erst dann bejaht werden, wenn den Nutzern durch den Einsatz von *Links* oder *Frames* ermöglicht wird, „beschränkende Massnahmen zu umgehen, die auf der Seite, auf der das geschützte Werk zu finden ist, getroffen wurden, um den Zugang der Öffentlichkeit [...] zu beschränken“<sup>1064</sup>. Hierunter sind sowohl Zugangsschranken (z.B. *paywalls*) als auch sämtliche Nutzungsschranken zu subsumieren, die dazu bestimmt und geeignet sind, um die Verlinkung von urheberrechtlich geschützten Werken zu unterbinden.<sup>1065</sup> Das Bestehen einer generellen Pflicht des *Link-Setzers* zur vorgängigen Abklärung, ob die ursprüngliche Zugänglichmachung des Werks rechtmässig erfolgt war, ist abzulehnen.<sup>1066</sup>

---

<sup>1062</sup> S.o. Rz. 59 ff.

<sup>1063</sup> S.o. Rz. 68.

<sup>1064</sup> EuGH vom 13. Februar 2014, Rechtssache C-466/12, Svensson, Rz. 31.

<sup>1065</sup> S.o. Rz. 74 f.

<sup>1066</sup> Vgl. dazu Rz. 77 f.



## II. Streaming aus der Perspektive der Nutzer

Unabhängig davon, welches Streaming-Verfahren eingesetzt wird, finden im 448  
 Rahmen der Werkwiedergabe urheberrechtlich relevante Vervielfältigungen  
 auf dem Nutzerrechner statt.<sup>1067</sup> Diese Zwischenspeicherungen werden im  
 Normalfall bereits nach kurzer Zeit wieder gelöscht bzw. mit neuen Daten  
 überschrieben. Damit beim Streaming das Vorliegen urheberrechtlich rele-  
 vanter Vervielfältigungen nach Art. 10 Abs. 1 lit. a URG nicht von techni-  
 schen Zufällen oder Einstellungen in der Wiedergabesoftware abhängig ist  
 und angesichts der Tatsache, dass sich der Umfang sowie die Bestandsdauer  
 der Teilvervielfältigungen nachträglich ohnehin nicht beweisen lassen, sollte  
 nicht auf die Schutzzfähigkeit des konkret zwischengespeicherten Werkteils  
 abgestellt werden. Vielmehr sollte „auch die sukzessive, chronologisch ge-  
 ordnete, auch nur flüchtige Vervielfältigung von an sich nicht schutzzfähigen  
 Werkteilen [als urheberrechtlich relevante Vervielfältigung aufgefasst wer-  
 den], solange in der Gesamtbetrachtung das ganze Werk oder schutzzfähige  
 Teile davon vervielfältigt werden“<sup>1068</sup>. Folglich sind sämtliche bei der  
 Werkwiedergabe mittels Streaming hergestellten transitorischen Vervielfälti-  
 gungen auf dem Nutzerrechner als urheberrechtlich relevante Vervielfälti-  
 gungen i.S.v. Art. 10 Abs. 2 lit. a URG zu qualifizieren.<sup>1069</sup> Ohne Einwilli-  
 gung der Rechteinhaber ist die Herstellung von Werkkopien nur dann zuläs-  
 sig, wenn sie von der Schranke für ausschliesslich technisch bedingte Ver-  
 vielfältigungen ohne eigenständige wirtschaftliche Bedeutung nach Art. 24a  
 URG oder einer anderen Schranke des Urheberrechts gedeckt werden.<sup>1070</sup>

Die Schrankenregelung von Art. 24a URG sieht vier Voraussetzungen vor, 449  
 die kumulativ erfüllt sein müssen. Das Kriterium der *flüchtigen oder beglei-  
 tenden Vervielfältigung* (lit. a) ist beim *True-On-Demand-Streaming* ohne  
 Weiteres zu bejahen, da die Kopie im Normalfall bereits kurze Zeit nach der  
 Wiedergabe wieder gelöscht bzw. überschrieben wird. Bei gewissen  
 Streaming-Verfahren – etwa dem *HTTP-Pseudo-Streaming* – werden tempo-  
 räre Vervielfältigungen auf den Nutzerrechnern hergestellt, die jedoch spä-  
 testens beim Schliessen des Browsers, oder dem Herunterfahren des Sys-  
 tems, gelöscht werden. Da der durchschnittliche Nutzer i.d.R. keine Kennt-

<sup>1067</sup> Ausführlich dazu Rz. 156 ff.

<sup>1068</sup> STOLZ, MMR 2013, 355; S.o. Rz. 163 ff.

<sup>1069</sup> S.o. Rz. 168 ff.

<sup>1070</sup> Vgl. dazu Rz. 172.

nis von diesen internen Speichervorgängen hat und ihm dadurch keine anderweitigen Nutzungsmöglichkeiten eröffnet werden, sollte auch hier das Vorliegen einer bloss begleitenden Vervielfältigung bejaht werden.<sup>1071</sup> Eine andere Bewertung drängt sich hingegen beim *Progressive Download* mit dauerhafter Speicherung auf, da hier – vergleichbar mit dem klassischen *Download* – das gesamte Werk heruntergeladen und auf dem Nutzerrechner abgespeichert wird. Diesfalls liegt auch keine bloss begleitende Vervielfältigung vor, weil diese nicht bloss beiläufig während des Streaming-Vorgangs hergestellt wurde, sondern gezielt angefertigt wurde, damit das Werk zu einem späteren Zeitpunkt auch offline abgerufen werden kann.<sup>1072</sup> Das Tatbestandserfordernis, dass die Vervielfältigung *integraler und wesentlich Teil eines technischen Verfahrens* sein muss (lit. b), ist beim Streaming i.d.R. erfüllt, da die vorübergehenden Vervielfältigungen im Nutzerrechner erforderlich sind um Schwankungen bei der Übertragungsrate (*Jitter*) auszugleichen, damit eine störungsfreie Werkwiedergabe gewährleistet ist.<sup>1073</sup> Gemäss Art. 24a lit. c URG sollen neben den *Access-Provider* auch die der rechtmässigen Nutzung dienenden Vervielfältigungen privilegiert werden. Damit sowohl die private als auch die berufliche Nutzung digitaler Werke möglich bleibt, ohne dass diese von ständigen Unsicherheiten betreffend deren Zulässigkeit begleitet werden, sollte das Tatbestandserfordernis der *rechtmässigen Nutzung* entsprechend weit ausgelegt werden, sodass sämtliche vorübergehenden Vervielfältigungen erfasst werden, die zur Wiedergabe digitaler Werke technisch notwendig sind (und zwar unabhängig von der Rechtmässigkeit der Quelle).<sup>1074</sup> Schliesslich fordert die Bestimmung von Art. 24a URG, dass die Vervielfältigung keine eigenständige wirtschaftliche Bedeutung haben darf (lit. d). Wann eine solche vorliegt, wird in der Lehre kontrovers diskutiert. Nach hier vertretender Ansicht kommt dem Tatbestandserfordernis der *eigenständigen wirtschaftlichen Bedeutung* keine über die Tatbestandsvoraussetzungen von Art. 24a lit. a-c URG hinausgehende Beschränkungsfunktion zu, weshalb *de lege ferenda* auch über eine ersatzlose Streichung dieses Tatbestandsmerkmals nachgedacht werden könnte.<sup>1075</sup>

- 450 Gestützt auf die in Art. 19 Abs. 1 lit. a URG statuierte Schranke des Privatgebrauchs sind im persönlichen Bereich und im Kreis von Personen, die

---

<sup>1071</sup> S.o. Rz. 174 ff.

<sup>1072</sup> Vgl. dazu Rz. 177.

<sup>1073</sup> Vgl. Rz. 178 ff.

<sup>1074</sup> S.o. Rz. 181 ff.

<sup>1075</sup> Zum Ganzen Rz. 192 ff.

unter sich eng verbunden sind, sämtliche Werkverwendungen an veröffentlichten Werken zulässig. Nach h.L. dürfen im Rahmen des Privatgebrauchs Vervielfältigungen geschützter Werke selbst dann hergestellt werden, wenn die Kopiervorlage aus einer unrechtmässigen Quelle stammt.<sup>1076</sup> Da innerhalb des Privatgebrauchs sogar die Herstellung dauerhafter Vervielfältigungen zulässig ist, werden dem *argumentum a maiore ad minus* folgend auch die vorübergehenden Vervielfältigungen beim Streaming von dieser Schrankenregelung umfasst.

### III. Technische Massnahmen zum Schutze digitaler Streaming-Angebote

Um digitale Werke gegen einen unerlaubten Zugriff bzw. eine unerlaubte Verwendung besser schützen zu können, setzen die Rechteinhaber technische Massnahmen ein. Diese lassen sich anhand ihrer Zweckbestimmung in Zugangs- und Nutzungsschranken unterteilen. Mit Zugangsschranken wird der Zugang zu urheberrechtlich geschützten Werken und anderen Schutzobjekten gesichert (z.B. durch Passwortsperren). Demgegenüber verfolgen Nutzungsschranken den Zweck, den Umfang der Werknutzung zu beschränken (etwa betreffend die Nutzungsdauer oder die Kopierbarkeit des Werks).<sup>1077</sup>

Die Umgehung wirksamer technischer Massnahmen wird durch Art. 39a Abs. 1 URG verboten.<sup>1078</sup> Sodann werden durch Abs. 3 von letztgenannter Bestimmung zahlreiche Vorbereitungshandlungen unter Strafe gestellt.<sup>1079</sup> Ziel der Strafbestimmung von Art. 69a Abs. 1 lit. b URG ist es, die Verbreitung von Umgehungswerkzeugen sowie das Erbringen von Dienstleistungen, die im Zusammenhang mit der Umgehung technischer Massnahmen stehen, zu unterbinden. Durch den in Art. 39a Abs. 4 URG statuierten Vorbehalt zugunsten von Umgehungshandlungen, die ausschliesslich dem Zweck gesetzlich erlaubter Verwendungen dienen, soll eine überschüssige Wirkung des Umgehungsschutzes gegenüber den Schrankenregelungen des Urheberrechts, verhindert werden. Die Tragweite dieses Vorbehalts ist insoweit einzuschränken, als nur Fälle der Umgehung technischer Massnahmen gem.

---

<sup>1076</sup> S.o. Rz. 203 ff.

<sup>1077</sup> S.o. Rz. 210 ff.

<sup>1078</sup> Vgl. Rz. 218 ff.

<sup>1079</sup> S.o. Rz. 224.

Art. 39a Abs. 1 URG erfasst werden, nicht aber Vorbereitungshandlungen nach Art. 39a Abs. 3 URG. Ausgehend vom Wortlaut der Bestimmung, welcher von einer „gesetzlich erlaubten Verwendung“ spricht, ergibt sich zudem, dass Art. 39a Abs. 4 URG nicht als Rechtfertigungsgrund bei der Umgehung von Zugangsschranken herangezogen werden kann. Die Umgehung von Zugangsschranken ist nicht als Werkverwendung zu qualifizieren, sondern stellt eine der Werkverwendung vorgelagerte Beschaffungshandlung dar. Ein Recht zur Umgehung von Zugangsschranken innerhalb des Privatgebrauchs kann m.E. aus Art. 39a Abs. 4 i.V.m. Art. 19 Abs. 1 lit. a URG nicht hergeleitet werden.<sup>1080</sup>

- 453 Eine Bestrafung des Täters wegen Umgehung einer wirksamen technischen Zugangsschranke nach den Strafbestimmungen des URG scheitert jedoch regelmässig an der missglückten Formulierung von Art. 69a Abs. 1 lit. a URG. Diese Bestimmung fordert kumulativ zur vorsätzlichen und unrechtmässigen Umgehung einer wirksamen technischen Massnahme, dass der Täter mit der Absicht handeln muss *eine gesetzlich unerlaubte Verwendung von Werken und anderen Schutzobjekten vorzunehmen*. Umgeht der Täter eine wirksame technische Massnahme ohne die Absicht (anschliessend) eine gesetzlich unerlaubte Verwendung am Werk vorzunehmen, entfällt eine Strafbarkeit nach Art. 69a Abs. 1 lit. a URG.<sup>1081</sup> Werden zur Umgehung von technischen Massnahmen Umgehungswerkzeuge i.S.v. Art. 39a Abs. 3 URG verwendet, ist das Vorliegen einer strafbaren Vorbereitungshandlung nach Art. 69a Abs. 1 lit. b URG zu prüfen.<sup>1082</sup>
- 454 Bei der Umgehung wirksamer Zugangssicherungen zu Datenangeboten sind zudem die einschlägigen Bestimmungen des StGB zu beachten.<sup>1083</sup> Anders als bei der urheberstrafrechtlichen Bestimmung von Art. 69a Abs. 1 lit. a URG, ist für die Strafbarkeit nach den Tatbeständen des StGB nicht vorausgesetzt, dass der Täter die Umgehung mit der Absicht vornimmt, *eine gesetzlich unerlaubte Verwendung von Werken oder anderen Schutzobjekten vorzunehmen*. Sodann zeitigt eine Straflosigkeit nach Art. 69a Abs. 1 lit. a URG wegen fehlendem Absichtserfordernis zur Vornahme einer unerlaubten Werkverwendung keine Reflexwirkung nach Art. 14 StGB auf eine etwaige Bestrafung gemäss den einschlägigen Bestimmungen des StGB, da die Um-

---

<sup>1080</sup> Zum Ganzen Rz. 225 ff.

<sup>1081</sup> S.o. Rz. 231.

<sup>1082</sup> Vgl. Rz. 232 f. und 299 ff.

<sup>1083</sup> Vgl. dazu Rz. 228 und Rz. 244 ff.

gehung von Zugangsschranken nicht vom Vorbehalt erlaubter Verwendungen nach Art. 39a Abs. 4 URG erfasst wird.<sup>1084</sup>

## IV. P2P-Streaming

Das *P2P-Streaming* stellt einen Sonderfall dar, da bei dieser Streaming- 455  
Technologie die heruntergeladenen Inhalte temporär auf dem Nutzerrechner zwischengespeichert und mittels *Upload* an andere Beteiligte innerhalb des Netzwerks weiterverbreitet werden. Das Hochladen geschützter Werke ohne Einwilligung der Rechteinhaber ist als unerlaubte Zugänglichmachung i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG zu qualifizieren. Sodann dienen die im Rahmen des *P2P-Streaming* im Nutzerrechner hergestellten Vervielfältigungen nicht bloss der Gewährleistung einer störungsfreien Werkwiedergabe. Vielmehr werden diese Kopien zum Zweck des *Filesharing* hergestellt, weshalb sie nicht als ausschliesslich technisch bedingte vorübergehende Vervielfältigungen i.S.v. Art. 24a URG zu qualifizieren sind. Weil das geschützte Werk bzw. Teile davon im Rahmen des *P2P-Streaming* i.d.R. gegenüber einer unbestimmten Zahl von Personen zugänglich gemacht wird, werden die Vervielfältigungen auch nicht von der Schrankenregelung zum Privatgebrauch gem. Art. 19 Abs. 1 lit. a URG erfasst. Sofern keine Einwilligung der Rechteinhaber vorliegt, erfüllen die Teilnehmer beim *P2P-Streaming* deshalb auch den Tatbestand der unerlaubten Herstellung von Werkexemplaren nach Art. 67 Abs. 1 lit. e URG.<sup>1085</sup>

Da die Anbieter der *P2P-Streaming-Software* die geschützten Werke nicht 456  
selbst hochladen, fällt eine Alleintäterschaft ausser Betracht. Angesichts des Tatbeitrags der Anbieter im Vorfeld der eigentlichen Urheberrechtsverletzung und im Ausführungsstadium ist eine Mittäterschaft denkbar. Die Anbieter wirken in massgebender Weise an den durch die Nutzer begangenen Urheberrechtsverletzungen mit – werden diese doch überhaupt erst durch die Software ermöglicht. Dadurch, dass die Anbieter um den Unterhalt der Software, die Auswahl der dargebotenen Inhalte und deren Darstellung besorgt sind, üben sie auch in der Ausführungsphase einen tragenden Einfluss aus. Da die *P2P-Streaming-Software* nahezu ausschliesslich zum Zwecke des illegalen *Filesharing* benutzt wird, war es für die Anbieter unstreitig

<sup>1084</sup> Siehe dazu Rz. 237 ff.

<sup>1085</sup> Vgl. Rz. 322 ff.

voraussehbar, dass die Software zur Begehung von Urheberrechtsverletzungen verwendet wird.<sup>1086</sup> Durch das Bereithalten der Software bringen die Anbieter zumindest konkludent zum Ausdruck, dass sie Urheberrechtsverletzungen i.S.v. Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG Vorschub leisten wollen.<sup>1087</sup>

- 457 Teilweise verfügen die *P2P-Streaming*-Programme über einen integrierten *VPN-Client*, der den Datenverkehr zwischen den beteiligten Nutzern anonymisiert. Durch die Zusicherung von Anonymität bei illegalem *Filesharing* wird motivierend auf die Nutzer eingewirkt am *P2P-Streaming* zu partizipieren. Mit Blick auf die beteiligten Anonymisierungsdienste ist daher eine psychische Gehilfenschaft zur Begehung von Urheberrechtsverstössen nach Art. 67 Abs. 1 lit. e und lit. g<sup>bis</sup> URG zu prüfen.<sup>1088</sup>

## V. Rechtsdurchsetzung bei Urheberrechtsverletzungen im Rahmen des Streaming

- 458 Eine Schutznorm an sich ist nichts wert, wenn sie prozessual nicht durchgesetzt werden kann. Damit die Strafbestimmungen des Urheberrechts im digitalen Umfeld nicht bloss toter Buchstabe bleiben muss sichergestellt werden, dass die Rechteinhaber bei Urheberrechtsverstössen wirksam gegen die Rechtsverletzer vorgehen können. Die derzeitige Rechtslage in der Schweiz ist unbefriedigend. Bei über das Internet begangenen Urheberrechtsverletzungen, verbleibt den Rechteinhabern häufig als einziger Anknüpfungspunkt die *IP-Adresse* des Anschlussinhabers, über welche die urheberrechtswidrige Handlung vorgenommen wurde. Seitdem das Bundesgericht im Logistep-Entscheid die Ermittlung von *IP-Adressen* durch Private als Persönlichkeitsverletzung i.S.v. Art. 12 Abs. 2 lit. a DSG qualifizierte und bei der Interessenabwägung nach Art. 13 Abs. 1 DSG die Interessen der betroffenen Anschlussinhaber stärker gewichtete als die Interessen der Rechteinhaber (und der Öffentlichkeit) an einer wirksamen Durchsetzung des Urheberrechts, ist

---

<sup>1086</sup> Im Unterschied zu anderen *Filesharing*-Programmen, liegt bei einer *P2P-Streaming-Software* nicht bloss eine entfernte, abstrakte Gefahr vor, dass diese nebst legalen Aktivitäten auch für illegales *Filesharing* genutzt wird.

<sup>1087</sup> Siehe Rz. 335 ff.

<sup>1088</sup> Vgl. Rz. 365 ff.

die strafrechtliche Verfolgung von Urheberrechtsverletzungen im Internet faktisch zum Erliegen gekommen.<sup>1089</sup>

Damit die Ermittlung von *IP-Adressen* durch Private zur Verfolgung von Urheberrechtsverletzungen im Internet künftig klar geregelt ist, wird vorgeschlagen, den Katalog mit Rechtfertigungsgründen nach Art. 13 Abs. 2 DSGVO um eine neue Bestimmung zu ergänzen. Diese soll es der bearbeitenden Person – unter Einhaltung der Bearbeitungsgrundsätze des EDÖB – gestatten, bei Urheberrechtsverletzungen im Internet die *IP-Adresse* des fehlbaren Nutzers aufzuzeichnen.<sup>1090</sup>

Als weitere Massnahme zur Bekämpfung des illegalen Filesharing im Internet schlägt die AGUR12 die Einführung eines Warnhinweismodells vor. Werden „schwerwiegende“ Urheberrechtsverletzungen durch die Nutzung von *P2P-Netzwerken* festgestellt, sollen die *Access-Provider* auf Hinweis der Rechteinhaber oder einer zuständigen Behörde hin einen einmaligen aufklärenden Hinweis an den Inhaber des hierzu verwendeten Internetanschlusses versenden. Durch den Warnhinweis soll der betroffene Internetanschlussinhaber über sein eigenes Fehlverhalten oder das Fehlverhalten etwaiger seiner Internetanschluss (mit-)benützenden Personen aufgeklärt werden. Zugleich wird der Anschlussinhaber zur Verhinderung einer „zivilrechtlichen Mithaftung im Wiederholungsfall“ verpflichtet, „den Weitergebrauch seines Anschlusses für Rechtsverletzungen über P2P-Netzwerke in angemessener Weise zu schützen“.<sup>1091</sup>

Gegen die Einführung eines Warnhinweismodells bei „schwerwiegenden“ Urheberrechtsverletzungen in *P2P-Netzwerken* spricht zunächst, dass hierdurch einzig über *P2P-Netzwerke* begangene Urheberrechtsverstöße erfasst werden und nicht auch solche, bei denen geschützte Werke über sog. *Filehoster* unerlaubt zugänglich gemacht werden. Diese Dienste haben sich längst zu einer valablen Alternative zum *P2P-Filesharing* entwickelt.<sup>1092</sup> Sodann würde durch die Einführung des vorgeschlagenen Warnhinweismodells eine Kausalhaftung für die Anschlussinhaber eingeführt, wenn über deren Internetzugänge wiederholt „schwerwiegende“ Urheberrechtsverletzungen ermittelt werden. Dadurch entfällt für die Rechteinhaber der oft nur schwer zu erbringende Nachweis, welcher Nutzer die in Frage stehende Ur-

---

<sup>1089</sup> S.o. Rz. 377 ff.

<sup>1090</sup> Vgl. dazu Rz. 401 ff.

<sup>1091</sup> Zum Ganzen Rz. 408 ff.

<sup>1092</sup> S.o. Rz. 421 ff.

heberrechtsverletzung zu verantworten hat, wenn verschiedene Personen gemeinsam einen Anschluss nutzen.<sup>1093</sup> Zugleich bedeutet dies aber eine Verschiebung der Haftung vom Urheberrechtsverletzer auf den Anschlussinhaber. Nach dem Prinzip „den Letzten beißen die Hunde“ kann dieser im Wiederholungsfall auch für Urheberrechtsverletzungen haftbar gemacht werden, die von einem Dritten begangen worden sind. Unklar ist dabei, wie sich der Anschlussinhaber von der Mithaftung befreien kann bzw. wie er seinen Internetanschluss „in angemessener Weise“ davor schützen soll, dass dieser nicht für die Begehung von Urheberrechtsverletzungen benützt wird. Eine Überwachung von sämtlichen seinen Anschluss mitbenützenden Personen ist dem Anschlussinhaber jedenfalls nicht zumutbar.<sup>1094</sup>

- 462 Des Weiteren schlägt die AGUR12 vor, dass *Hosting-Provider* auf Anzeige der Rechteinhaber oder einer zuständigen Behörde hin unerlaubt hochgeladene Inhalte von ihren Servern entfernen müssen (*take down*). An diesem Vorschlag ist zu kritisieren, dass im Rahmen des Privatgebrauchs nach Art. 19 Abs. 1 lit. a URG auch geschützte Werke auf virtuelle Speicherdienste im Internet hochgeladen werden dürfen. Nur wenn die hochgeladenen Werke unerlaubt i.S.v. Art. 67 Abs. 1 lit. g<sup>bis</sup> URG zugänglich gemacht werden, liegt eine Urheberrechtsverletzung vor.<sup>1095</sup>
- 463 Jene *Hosting-Provider*, deren Geschäftsmodelle offensichtlich auf Rechtsverletzungen durch die Nutzer angelegt sind, oder welche die Gefahr einer rechtsverletzenden Nutzung absichtlich fördern, sollen nach Ansicht der AGUR12 auf Anzeige der Rechteinhaber hin unerlaubte Inhalte entfernen und „das erneute unerlaubte Hochladen solcher Inhalte im Rahmen des Zumutbaren verhindern“. Eine Verpflichtung der *Filehoster*, das wiederholte Hochladen von geschützten Werken zu verhindern (*stay down*), ist in verschiedener Hinsicht zu beanstanden. Zunächst können die *Filehoster* nicht verhindern, dass eine gelöschte Datei erneut hochgeladen wird.<sup>1096</sup> Weiter liegt erst dann eine Urheberrechtsverletzung vor, wenn die erneut hochgeladene Datei wiederholt unerlaubt zugänglich gemacht wird.<sup>1097</sup> Letztlich können die *Filehoster* auch durch aufwendige Kontrollen von *Linksammlungen* keine zukünftigen Urheberrechtsverletzungen verhindern, sondern lediglich

---

<sup>1093</sup> Zwischen Anschlussinhaber und Rechtsverletzer muss keine Identität bestehen; vgl. auch BAUMGARTNER, 207 und 210.

<sup>1094</sup> Vgl. Rz. 413 ff.

<sup>1095</sup> S.o. Rz. 423.

<sup>1096</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 64, m.w.H.

<sup>1097</sup> S.o. Rz. 423 und Rz. 462.



bestehende Rechtsverletzungen beseitigen.<sup>1098</sup> Eine Verpflichtung der *Filehoster* zur umfassenden Kontrolle sämtlicher *Linksammlungen* ist bereits wegen der fehlenden technischen Umsetzbarkeit abzulehnen.<sup>1099</sup>

Zielführender wäre m.E. eine Beschränkung der *Filesharing-Funktionen* bei *Filehosting-Diensten* auf eine bestimmte Anzahl *Downloads* oder Streams, die mit dem Privatgebrauch nach Art. 19 Abs. 1 lit. a URG korrespondiert.<sup>1100</sup> Dies liesse sich durch die Einrichtung eines Content-ID-Systems erreichen, das die hochgeladenen Inhalte nach urheberrechtlich geschützten Werken durchsucht und dabei automatisch die Zahl möglicher *Downloads* oder simultaner Stream-Abrufe limitiert.<sup>1101</sup>

Schliesslich schlägt die AGUR12 vor, dass die *Access-Provider* – auf behördliche Anweisung hin – den Zugang zu Portalen, deren Inhalte aus „offensichtlich rechtswidrigen Quellen“ angeboten werden, mittels IP- und DNS-Blocking sperren sollen. Gegen die Einführung von DNS- und IP-Sperren spricht zunächst, dass diese relativ einfach umgangen werden können. Besonders bei IP-Sperren besteht zudem ein erhebliches Risiko, dass auch legale Inhalte mitgesperrt werden (*Overblocking*). Angesichts der Schwere des Eingriffs in die Grundrechte der Betroffenen ist es zudem problematisch, dass die vorgeschlagenen Sperrmassnahmen ohne vorgängige richterliche Prüfung verhängt werden können. Deshalb sollten DNS- und IP-Sperren nur mit grosser Zurückhaltung und einzig in schwerwiegenden Fällen eingesetzt werden.<sup>1102</sup>

---

<sup>1098</sup> BERANEK ZANON, Jusletter IT vom 11. Dezember 2013, Rz. 64 und Rz. 115, weist zutreffend darauf hin, dass i.d.R. im Zeitpunkt der Veröffentlichung des *Links* „die *Verletzung bereits begangen* [ist], sie kann damit nicht mehr verhindert werden“.

<sup>1099</sup> Vgl. Rz. 425 ff.

<sup>1100</sup> Wird etwa ein geschütztes Musikstück oder Filmwerk hundertfach heruntergeladen oder gleichzeitig von zwanzig Personen mittels Streaming-Verfahren konsumiert, ist diese Zahl m.E. nicht mehr mit dem zulässigen Privatgebrauch begründbar.

<sup>1101</sup> Siehe Rz. 428 ff.

<sup>1102</sup> Vgl. Rz. 429 ff.

## VI. Der weitere Gesetzgebungsprozess seit Dezember 2015

- 466 Nachfolgend sollen die wichtigsten Eckpunkte der geplanten Revision des Urheberrechtsgesetzes zusammengefasst werden. Im Fokus stehen dabei die Massnahmen zur Bekämpfung der Internetpiraterie.

### 1. Vorentwurf zur Änderung des URG

- 467 Im Dezember 2015 präsentierte der Bundesrat gestützt auf den Schlussbericht der AGUR12 einen Vorentwurf für die Gesetzesrevision, welcher bis Ende März 2016 in die Vernehmlassung ging.<sup>1103</sup>

#### A. Teilnehmeridentifikation und Warnhinweismodell

- 468 Als Massnahme zur Pirateriebekämpfung sah der Vorentwurf unter anderem ein Verfahren zur Identifikation und Verfolgung von Teilnehmerinnen und Teilnehmern bei Urheberrechtsverletzungen über *Peer-to-Peer-Netzwerke* im Internet vor. In einem ersten Schritt sollten IP-Adressen von Teilnehmerinnen und Teilnehmern in *Peer-to-Peer-Netzwerken* gesammelt werden, über deren Internetzugänge mutmasslich schwerwiegende Urheberrechtsverletzungen begangen wurden (Art. 66j E-URG 2015). Die Zugangsprovider sollten nach Art. 66g E-URG 2015 dazu verpflichtet werden, den Inhabern der betroffenen Internetanschlüsse zunächst aufklärende Warnhinweise zuzustellen. Diese Warnhinweise sollten die betroffenen Anschlussinhaber über die Rechtslage sowie die Folgen der Nichtbeachtung der Warnhinweise informieren. Falls über denselben Internetanschluss trotz zweimaliger Zustellung eines Warnhinweises innerhalb von zwölf Monaten eine erneute Urheberrechtsverletzung festgestellt wird, soll das Zivilgericht auf Antrag eines Urhebers die Identifikation des betroffenen Anschlussinhabers über die IP-Adresse anordnen (Art. 62a E-URG 2015).<sup>1104</sup>

---

<sup>1103</sup> <<https://www.ejpd.admin.ch/ejpd/de/home/aktuell/themen/urg.html>> (besucht 25. Februar 2018).

<sup>1104</sup> Hierdurch soll dem Urheber ermöglicht werden, in einem nächsten Schritt zivilrechtliche Schritte zur Rechtsdurchsetzung gegen den betroffenen Anschlussinhaber einzuleiten.

## **B. Take down und stay down Pflicht für Hosting Provider**

Gemäss Art. 66b E-URG 2015 sollten die Hosting Provider dazu verpflichtet werden – auf Mitteilung der in ihrem Urheber- oder verwandten Schutzrecht verletzten Person bzw. einer zuständigen Behörde – den Zugang zu mutmasslich widerrechtlich öffentlich zugänglich gemachten Werken oder andern Schutzobjekten zu sperren oder diese von ihren Servern zu entfernen („take down“). Weiter sollte der betroffene Hosting Provider dazu verpflichtet werden, den mutmasslich fehlbaren Nutzer über den „take down“ zu informieren und ihn auf die Möglichkeit des Widerspruchs und dessen Folgen aufmerksam zu machen. Falls ein Inhabitant mit Zustellungsdomizil in der Schweiz Widerspruch gegen einen solchen „take down“ erheben sollte, sollte der Zugang zum gesperren Werk oder anderen Schutzobjekt widerhergestellt werden, bis die Angelegenheit entweder zwischen den betroffenen Personen oder durch die Gerichte geklärt ist. Hierfür soll die Identität des Inhabitant gegenüber der mitteilenden Person bekannt gegeben werden, damit diese zivilrechtliche Schritte gegen den mutmasslich rechtswidrigen Anbieter von urheberrechtlich geschützten Inhalten einleiten kann. Wenn kein Widerspruch erhoben wird, sah Art. 66b Abs. 4 i.V.m. Art. 66c E-URG 2015 vor, dass denjenigen Hosting Providern, die keiner Selbstregulierungsorganisation angeschlossen sind, die Pflicht auferlegt werden soll, im Rahmen des technisch und wirtschaftlich Zumutbaren zu verhindern, dass ein unerlaubt zugänglich gemachtes Werk oder anderes Schutzobjekt erneut über ihre Server unerlaubt zugänglich gemacht wird („stay down“).<sup>1105</sup> 469

## **C. Netzsperrern**

In Art. 66d E-URG 2015 war eine Zugangssperre zu von ausländischen Anbietern urheberrechtswidrig zugänglich gemachten Werken vorgesehen. In einem ersten Schritt sollte die in ihren Urheberrechten mutmasslich verletzte Person beim Institut für geistiges Eigentum (IGE) die Sperrung des Zugangs zum entsprechenden Angebot verlangen. Kann die in ihren Urheberrechten verletzte Person die Voraussetzungen gemäss Art. 66d Abs. 2 lit. a-d E-URG 2015 glaubhaft machen, sollte das IGE eine Sperrung des Zugangs zum entsprechenden Angebot verfügen, indem der betroffene Anbieter auf eine sog. 470

---

<sup>1105</sup> Gemäss Art. 66c Abs. 1 E-URG 2015 waren Hosting Provider, deren Geschäftsmodell „auf der Förderung systematischer Urheberrechtsverletzungen aufbaut“, vom Anschluss an eine Selbstregulierungsorganisation ausgeschlossen.

Sperrliste gesetzt wird.<sup>1106</sup> Die Internetzugangsanbieter („Access-Provider“) sollten dazu verpflichtet werden, sämtliche Zugriffe auf gesperrte Internetseiten auf einen vom IGE betriebenen Server umzuleiten, über welchen die Teilnehmer informiert werden, dass der Zugang auf das abgefragte Angebot gesperrt wurde. Gemäss dem erläuternden Bericht war zur technischen Umsetzung primär der Einsatz von IP- oder DNS-Blocking vorgesehen.<sup>1107</sup>

## **2. Ergebnis der Vernehmlassung und Kompromiss in der AGUR12 II**

- 471 In der Vernehmlassung stiess die Vorlage auf starken Widerstand und es zeichnete sich keine mehrheitsfähige Lösung ab.<sup>1108</sup> Mit dem Ziel eine kompromissfähige Lösung zu finden wurde im August 2016 die AGUR12 II einberufen, welche neu durch zwei Providervertreter sowie einen Vertreter des Bundesamtes für Justiz erweitert wurde.<sup>1109</sup> Die AGUR12 II beendete ihre Arbeit im März 2017.<sup>1110</sup>

### **A. Mehr Pflichten für Hosting Provider**

- 472 Beim zentralen Thema der Pirateriebekämpfung einigte sich die AGUR12 II auf eine Kompromisslösung, die neue Pflichten für Hosting Provider vorsah. Schweizer Hosting Provider sollen bei über ihre Server begangenen Urheberrechtsverletzungen dazu verpflichtet werden, die betroffenen Inhalte zeitnah zu löschen („*take down*“). Schafft ein Hosting Provider darüber hinaus eine besondere Gefahr für die Begehung von Urheberrechtsverletzungen, hat er zudem dafür zu sorgen, dass einmal beseitigte Urheberrechtsverletzungen „*take down*“ auch beseitigt bleiben („*stay down*“).<sup>1111</sup>

---

<sup>1106</sup> Gegen die Sperrverfügung war ein Einspracheverfahren vorgesehen (Art. 66e Abs. 2 E-URG 2015).

<sup>1107</sup> Erläuternder Bericht 2015, 75.

<sup>1108</sup> <<https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2016/2016-12-022/ve-berd.pdf>> (besucht 25. Februar 2018).

<sup>1109</sup> <<https://www.ejpd.admin.ch/ejpd/de/home/aktuell/themen/urg.html>> (besucht 25. Februar 2018).

<sup>1110</sup> <[https://www.ige.ch/fileadmin/user\\_upload/recht/national/d/urheberrecht/AGUR12\\_II\\_Medienmitteilung\\_20170302\\_DE.pdf](https://www.ige.ch/fileadmin/user_upload/recht/national/d/urheberrecht/AGUR12_II_Medienmitteilung_20170302_DE.pdf)> (besucht 25. Februar 2018).

<sup>1111</sup> <[https://www.ige.ch/fileadmin/user\\_upload/recht/national/d/urheberrecht/AGUR12\\_II\\_Medienmitteilung\\_20170302\\_DE.pdf](https://www.ige.ch/fileadmin/user_upload/recht/national/d/urheberrecht/AGUR12_II_Medienmitteilung_20170302_DE.pdf)> (besucht 25. Februar 2018).

## **B. Datenbearbeitung zur strafrechtlichen Verfolgung von Urheberrechtsverletzungen im Internet**

Um die strafrechtliche Verfolgung von Urheberrechtsverletzern zu ermöglichen, verlangte die AGUR12 II eine ausdrückliche Klarstellung der Zulässigkeit der hierfür notwendigen Datenbearbeitungen.<sup>1112</sup> 473

## **C. Abkehr von Netzsperrern und Warnhinweismodell**

Die im Vorentwurf zum revidierten Urheberrechtsgesetz vorgeschlagene Einführung von Netzsperrern zu urheberrechtsverletzenden ausländischen Angeboten durch die Internetzugangsanbieter war in der Kompromisslösung der AGUR12 II nicht mehr enthalten. Ebenso ersatzlos gestrichen wurde die Einführung eines Warnhinweismodells bei schwerwiegenden Urheberrechtsverletzungen über *Peer-to-Peer-Netzwerke* („P2P-Netzwerke“).<sup>1113</sup> 474

## **3. Gesetzesentwurf und Botschaft zur Revision des Urheberrechtsgesetzes**

Am 22. November 2017 verabschiedete der Bundesrat die Botschaft zur Änderung des Urheberrechtsgesetzes.<sup>1114</sup> 475 Die Botschaft und der Gesetzesentwurf wurden für die parlamentarische Beratung an den National- und Ständerat überwiesen.

## **A. Stay down-Regel für gewisse Hosting Provider**

Im Gesetzesentwurf wurde die „stay down“-Regel in den Art. 39d und Art. 62 Abs. 1<sup>bis</sup> E-URG 2017 verankert. Diese Bestimmung richtet sich nicht gegen sämtliche Anbieter von Online-Speicherdiensten, sondern hat gezielt jene Hosting Provider im Visier, von deren Geschäftsmodellen eine 476

---

<sup>1112</sup> <[https://www.ige.ch/fileadmin/user\\_upload/recht/national/d/urheberrecht/AGUR12\\_II\\_Medienmitteilung\\_20170302\\_DE.pdf](https://www.ige.ch/fileadmin/user_upload/recht/national/d/urheberrecht/AGUR12_II_Medienmitteilung_20170302_DE.pdf)> (besucht 25. Februar 2018).

<sup>1113</sup> In der Vernehmlassung wurde das Warnhinweismodell von einer Mehrheit abgelehnt, weil es als unverhältnismässig, zu kompliziert und zu aufwändig betrachtet wurde; Erläuternder Bericht, 17 ff.

<sup>1114</sup> <<https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-11-221.html>> (besucht 25. Februar 2018).

besondere Gefahr für die Begehung von Urheberrechtsverletzungen ausgeht.<sup>1115</sup>

- 477 Durch Art. 39d E-URG 2017 werden die Betreiber solcher Hosting Provider dazu verpflichtet, zu verhindern, dass ein Werk oder anderes Schutzobjekt Dritten mithilfe desselben Dienstes erneut widerrechtlich zugänglich gemacht wird („*stay down*“).<sup>1116</sup>
- 478 Die Wahl der Massnahmen zur technischen Umsetzung der „*stay down*“-Pflicht wird dem betroffenen Hosting Provider überlassen. Gemäss Art. 39d Abs. 2 E-URG 2017 hat der betroffene Hosting Provider jene Massnahmen zu ergreifen, die ihm unter Berücksichtigung der Gefahr solcher Rechtsverletzungen technisch und wirtschaftlich zuzumuten sind. Der Umfang dieser Pflicht ist unter Berücksichtigung der Umstände im konkreten Einzelfall festzulegen und variiert insbesondere in Abhängigkeit von Speicherkapazität, Grösse und Professionalität des Hosting Providers.<sup>1117</sup>
- 479 Trifft ein Hosting Provider keine oder bloss ungenügende Massnahmen, um das erneute unerlaubte Zugänglichmachen eines geschützten Werks zu verhindern, können die Rechtsinhaber vom Gericht verlangen, eine drohende Verletzung zu verbieten (Art. 62 Abs. 1 lit. a URG i.V.m. Art. 62 Abs. 1<sup>bis</sup> und Art. 39d E-URG 2017).<sup>1118</sup>

---

<sup>1115</sup> Nach Art. 39d lit. c E-URG 2017 liegt eine besondere Gefahr vor, wenn ein Hosting Provider durch die technische Funktionsweise seines Dienstes oder durch dessen wirtschaftliche Ausrichtung die Begehung von Urheberrechtsverletzungen begünstigt. Eine solche besondere Gefahr dürfte regelmässig von gewissen sog. Sharehostern ausgehen, die ihren Nutzern für den Upload besonders gefragter Inhalte eine Belohnung anbieten. Weil aktuelle geschützte Werke bekanntermassen besonders häufig gesucht und abgerufen werden, wurden mit solchen Belohnungen Anreize für die Begehung von Urheberrechtsverletzungen geschaffen. Bisher war es gängige Praxis, dass die Sharehoster nach Aufforderung der Rechteinhaber das über ihren Dienst unerlaubt zugänglich gemachte Werk zwar gelöscht haben, dieses aber meist innert kurzer Zeit wieder verfügbar war (etwa weil ein anderer Nutzer das betreffende Werk erneut hochgeladen hatte). Tritt Art. 39d E-URG 2017 in Kraft, haftet der betroffene Sharehoster im Wiederholungsfall auch dann, wenn das betroffene Werk ohne sein Wissen von einem seiner Nutzer erneut hochgeladen und durch Veröffentlichung des entsprechenden Links unerlaubt zugänglich gemacht wird.

<sup>1116</sup> Botschaft URG 2017, 634 f.; Gemäss Botschaft soll durch die „*stay down*“-Pflicht sichergestellt werden, dass Unterlassungsansprüche gegen Hostingprovider, die eine besondere Gefahr von Urheberrechtsverletzungen schaffen, durchgesetzt werden können.

<sup>1117</sup> Vgl. zum Ganzen Botschaft URG 2017, 637.

<sup>1118</sup> Botschaft URG 2017, 637.

## **B. Bearbeitung von Personendaten zum Zweck der Strafantragstellung oder der Strafanzeigeerstattung**

Mit Art. 77i E-URG 2017 soll eine ausdrückliche gesetzliche Grundlage für die Datenbearbeitung zur strafrechtlichen Verfolgung von Urheberrechtsverletzungen im Internet geschaffen werden.<sup>1119</sup> Diese Bestimmung sieht vor, dass Rechtsinhaber, die in ihren Urheberrechten oder verwandten Schutzrechten verletzt werden, Personendaten bearbeiten dürfen, soweit dies zum Zweck der Strafantragsstellung oder der Strafanzeigeerstattung notwendig ist und sie rechtmässig darauf zugreifen können. Diese Daten dürfen auch für die adhäsionsweise Geltendmachung von zivilrechtlichen Ansprüchen oder für deren Geltendmachung nach abgeschlossenem Strafverfahren verwendet werden.<sup>1120</sup> Gemäss Art. 77i Abs. 2 E-URG 2017 sind die Rechtsinhaber verpflichtet, den Zweck Datenbearbeitung, die Art der bearbeiteten Daten und den Umfang der Datenbearbeitung offenzulegen.

## **C. Keine Netzsperrern und keine Kriminalisierung des Konsums illegaler Angebote**

Die im Vorentwurf geplante Einführung einer gesetzlichen Regelung für die Sperrung von ausländischen Webseiten, auf denen illegal urheberrechtlich geschützte Inhalte angeboten werden, stiess in der Vernehmlassung auf starke Ablehnung und erwies sich als nicht mehrheitsfähig, weshalb im Gesetzesentwurf auf Netzsperrern durch die Access Provider verzichtet wurde.<sup>1121</sup> Ebenso wurde davon abgesehen, den Privatkonsum von urheberrechtlich geschützten Werken aus einer illegalen Quelle zu pönalisieren.

---

<sup>1119</sup> Botschaft URG 2017, 601; Im Logistep-Entscheid hatte das Bundesgericht festgehalten, dass das Sammeln von IP-Adressen durch Vertreter der Rechtsinhaber nicht mit dem DSG vereinbar sei. Diese Rechtsprechung soll durch Art. 77i E-URG 2017 aufgehoben werden. Gestützt auf diese Bestimmung können die Rechtsinhaber IP-Adressen von Teilnehmern sammeln, um mutmassliche Urheberrechtsverletzungen zu dokumentieren. Die gesammelten Daten werden anschliessend an die Strafverfolgungsbehörden zur Einleitung eines Strafverfahrens weitergeleitet.

<sup>1120</sup> Wird ein Strafverfahren einzig für die anschliessende Durchsetzung von zivilrechtlichen Ansprüchen angestossen, könnte dies als Umgehung taxiert werden. Gemäss dem in der Vernehmlassung verworfenen Art. 62a E-URG 2015 war hingegen noch vorgesehen, dass der Rechtsinhaber bei schwerwiegenden Urheberrechtsverletzungen über P2P-Netzwerke die Identifizierung des betroffenen Anschlussinhabers auf Anordnung eines Zivilgerichts verlangen konnte, um gegen diesen zivilrechtlich vorzugehen.

<sup>1121</sup> Botschaft URG 2017, 613.

## **D. Weitere Streaming-relevante Änderungen**

### **a) *Video-on-Demand Vergütung für Urheber und Interpreten***

- 482 In der Vernehmlassung wurde die Einführung eines nichtabtretbaren Vergütungsanspruchs für Filmurheber und Filmschauspieler gegenüber den Anbietern von Video-on-Demand Angeboten gefordert.<sup>1122</sup> Hierfür wurde argumentiert, dass die Online-Nutzungen von Werken in der Vergangenheit stark gestiegen seien, ohne dass die Filmurheber und Schauspieler von diesem Umstand profitieren konnten.<sup>1123</sup> Die geltende Rechtslage soll deshalb um eine Vergütungspflicht für Video-on-Demand Angebote erweitert werden. Die Beteiligungen an den Einnahmen aus der Online-Verwertung sollen nach Art. 13a und Art. 35a E-URG 2017 durch die Verwertungsgesellschaften wahrgenommen werden.<sup>1124</sup> Die Anbieter von Video-on-Demand Angeboten schulden dabei einerseits eine an die Produzenten zu entrichtende Lizenzgebühr sowie andererseits die über die Verwertungsgesellschaften an die Urheber fliessenden Entschädigungen.<sup>1125</sup>

### **b) *Verlängerung der Schutzfrist im Bereich der verwandten Schutzrechte***

- 483 Durch den geänderten Art. 39 Abs. 1 E-URG 2017 soll die Schutzfrist für die ausübenden Künstlerinnen und Künstler sowie für die Herstellerinnen und Hersteller von Ton- und Tonbildträgern von derzeit 50 Jahren auf neu 70 Jahre verlängert werden. Dadurch sollen die Kunstschaftenden länger an der Verwertung ihrer künstlerischen Tätigkeit beteiligt werden.<sup>1126</sup>

---

<sup>1122</sup> Erläuternder Bericht 2015, 25; Gemäss Botschaft URG 2017, 604, soll sich das System der Video-on-Demand Vergütung auf Filme von Schweizer Produzentinnen und Produzenten beschränken sowie auf Filme, die einen kollektiv wahrzunehmenden Vergütungsanspruch vorsehen.

<sup>1123</sup> Von Art. 13 URG ist nur die Vergütungspflicht für das Vermieten von Werkexemplaren erfasst. Mittlerweile hat das Verleihmodell von Videotheken angesichts der zahlreichen Onlineanbieter stark an Bedeutung verloren; vgl. dazu <<http://blog.suisa.ch/de/urheber-rechtsrevision-die-urheber-und-verleger-muessen-von-der-online-nutzung-ihrer-werke-besser-profitieren/>> (besucht 25. Februar 2018).

<sup>1124</sup> Botschaft URG 2017, 621 ff. und 632 f.

<sup>1125</sup> Erläuternder Bericht 2015, 25.

<sup>1126</sup> Gemäss Botschaft URG 2017, 603, wird das Erfordernis einer Verlängerung der Schutzdauer damit begründet, dass die Interpretinnen und Interpreten gewöhnlich ihre Laufbahn in relativ jungen Jahren beginnen und daher ihre Darbietungen bei der ge-



#### 4. Fazit zur Botschaft zur Revision des Urheberrechts

Es ist m.E. zu begrüßen, dass der Bundesrat in seiner Botschaft und im Entwurf auf die Einführung eines Warnhinweismodells sowie auf Netzsperrern verzichtet. Die Erfahrungen mit Warnhinweismodellen im Ausland belegen, dass diese Massnahme einen unverhältnismässig grossen Verwaltungsaufwand nach sich zieht und weiter zu einer ungerechten Kausalhaftung des Anschlussinhabers führt.<sup>1127</sup> Der Verzicht auf die von der Musik- und Filmindustrie geforderten Netzsperrern für ausländische Webseiten, auf denen illegal urheberrechtlich geschützte Inhalte angeboten werden, ist m.E. richtig, da hierdurch das illegale Angebot nicht gelöscht, sondern lediglich gesperrt wird.<sup>1128</sup> Sodann war problematisch, dass gemäss dem Vorentwurf die Netzsperrern nicht durch ein staatliches Gericht, sondern durch das IGE verfügt werden sollten.<sup>1129</sup> Schliesslich sind Netzsperrern auch bloss beschränkt wirksam, da sie relativ einfach umgangen werden können.

Wie bis anhin bleibt der private Download aus illegaler Quelle straffrei. Dies ist zu befürworten, da hier die Schrankenregelung zugunsten des Privatgebrauchs greift und es für den Konsumenten im Einzelfall oft gar nicht ersichtlich ist, ob vom Anbieter die notwendigen Einwilligungen für das Zugänglichmachen der geschützten Inhalte eingeholt worden sind.

Durch die in der Botschaft vorgesehenen Regelung für die Datenbearbeitung zur strafrechtlichen Verfolgung von Urheberrechtsverletzungen soll neu eine genügende gesetzliche Grundlage für die Überwachung der Urheberrechtsverletzungen im Internet, etwa in P2P-Netzwerken, geschaffen werden. Da insgesamt das Phänomen der „Tauschbörsen“ im Internet zunehmend an

---

genwärtigen Schutzdauer von 50 Jahren gegen Ende ihres Lebens regelmässig ungeschützt sind, woraus eine Einkommenlücke resultiert.

<sup>1127</sup> Die Einführung eines Warnhinweismodells für „schwerwiegende Urheberrechtsverletzungen in P2P-Netzwerken“ hätte auch weitreichende Konsequenzen für die Betreiber von Internet-Hotspots, da diese die Internetaktivitäten ihrer Nutzer nicht überwachen können und der Hinweis in den AGBs, dass der Dienst nicht für illegales Filesharing missbraucht werden darf, für eine Haftungsbefreiung nicht ausreichen dürfte.

<sup>1128</sup> Eine Alternative dazu bietet der sog. „Follow the Money“-Ansatz, bei dem die Geldflüsse der Werbeeinnahmen verfolgt und entsprechende Konten trockengelegt werden; siehe dazu: <<https://www.engadget.com/2016/07/21/kickasstorrents-apple-facebook-homeland-security/>> (besucht 25. Februar 2018).

<sup>1129</sup> Erläuternder Bericht 2015, 76.

Relevanz verliert, ist m.E. die Gefahr von Massenabmahnungen als nicht besonders hoch einzustufen.

- 487 Die sog. „*stay down*“-Verpflichtung richtet sich ausschliesslich gegen jene Hosting Provider, von denen eine „besondere Gefahr“ für die Begehung von Urheberrechtsverletzungen ausgeht. Solange eine solche „besondere Gefahr“ mit der gebotenen Zurückhaltung beurteilt und einzig in klaren Fällen bejaht wird, spricht m.E. nichts dagegen, dass solche Hosting Provider im Wiederholungsfall für die über ihre Server begangenen Urheberrechtsverletzungen zur Verantwortung gezogen werden können.
- 488 Nach hier vertretener Auffassung sind die in der Botschaft und im Entwurf präsentierten Neuerungen als ausgewogene Kompromisslösung zu bewerten. Der Bundesrat hat m.E. gut daran getan, bei der Bekämpfung der Internetpiraterie auf die besonders umstrittenen Punkte zu verzichten. Es liegt nicht im Interesse des Urheberrechts, wenn neue Regeln geschaffen werden, die in der Praxis nicht oder nur mit unverhältnismässigem Aufwand durchgesetzt werden können. Zugleich stimmt optimistisch, dass etwa das Problem des illegalen Filesharing mittlerweile gerade auch wegen der Zunahme an attraktiven legalen Alternativen zunehmend an Bedeutung verliert.<sup>1130</sup>
- 489 Das Parlament hat den Entwurf nun zu beraten. Der Umstand, dass über die Modernisierung des Schweizer Urheberrechts seit dem Jahr 2011 diskutiert wird und die heftige Kritik, welche bereits der Vorentwurf im Vernehmlassungsverfahren hatte einstecken müssen, zeigen eindrücklich, wie weit die Meinungen der involvierten Parteien teilweise auseinandergehen. Vor diesem Hintergrund ist es daher weiterhin offen, ob dieser Kompromiss die Beratungen überstehen wird.

---

<sup>1130</sup> Aus Sicht der grossen Mehrheit der Künstler vermögen allerdings die geringen Vergütungen, welche die Streaming-Dienste etwa pro gespielter Musikstück bezahlen, den Wegfall aus den Verkäufen von physischen Tonträgern oder Bezahl-Downloads nicht zu kompensieren. Um einen Dollar zu verdienen muss ein Werk beispielsweise auf YouTube beinahe 1000 Mal angeklickt werden, bei Spotify werden etwa 140 Klicks benötigt und bei Apple weniger als 100 Abrufe; vgl. dazu <<https://www.nzz.ch/finanzen/neue-hoergewohnheiten-die-musik-stroemt-das-geld-nicht-ld.145130>> (besucht 25. Februar 2018).



## **Lebenslauf**

Ich wurde am 11. Mai 1986 in Zürich geboren. Ich besuchte in Zürich die Kantonsschule Hottingen, welche ich im Jahr 2006 abschloss. Im September 2007 begann ich mein Studium an der Rechtswissenschaftlichen Fakultät der Universität Zürich und erwarb im März 2013 den Master of Law UZH. Darauf war ich bis Oktober 2015 als wissenschaftlicher Assistent und Doktorand am Lehrstuhl von Prof. Dr. iur Christian Schwarzenegger tätig.